جريمة التجسس المعلوماتي

- دراسة مقارنة -



ضرغام جابر عطوش آل مواش
ماجستير القانون الجنائي



مكتبة دار السلام القانونية

جريمة التجسس
المعلوماتي

جريمة التجسس المعلوماتي

«دراسة مقارنة»

ضرغام جابر عطوش آل مواش

ماجيستير القانون الجنائي

الطبعة الأولى

2017 - 1438





ح المركز العربي للدراسات والبحوث العلمية للنشر والتوزيع، 2017م

آل مواش ، ضرغام جابر عطوش

جريمة التجسس المعلوماتي : دراسة مقارنة / ضرغام جابر عطوش آل مواش؛ اشراف إسراء محمد علي سالم الأسدي .

- قليوب : المركز العربي للدراسات والبحوث العلمية ٢٠١٦.

.. ص ؛ ..سم

اطروحة (ماجيستير في القانون الجنائي) معهد العلمين للدراسات العليا

ردمك: 978-977-6567-25-2

1 -الجرائم الحاسوبية

2 - أمن المعلومات

3. الحاسوبات الألكترونية - قوانين وتشريعات

ديوي 364.168

رقم الإيداع: 2016/16883


ISBN 978-977-6567-25-2



جمهورية مصر العربية

القاهرة - شبرا - 3
شارع ترعة النصراني أمام
مسجد التقوى - منطي
- شبرا الخيمة

00(20) 1282441890

00(20) 233518784

yasser261098@gmail.

www. ACBOOkZONE.COM



العراق - النجف الأشرف

شارع الإمام علي - مقابل

الجامعة الإسلامية

- 07711480962

07803012166

hideraljassme@gmail.com



﴿وَلَا تَجَسَّسُوا﴾

صَدَقَ اللهُ العَظِيم

(سورة الحجرات: من الآية 11)

﴿إِلَّا مَنِ اسْتَرَقَ السَّمْعَ فَأَتْبَعَهُ شِهَابٌ مُبِينٌ﴾

صَدَقَ اللهُ العَظِيم

(سورة الحجر: الآية 18)

الاهداء

الى من بلغ الرسالة وأدى الامانة...نبي الرحمة محمد بن عبد الله (ﷺ)

الى سيد الشهداء الحسين بن علي (عليه السلام)..الذي بذل نفسه ونفوس أهل بيته لنصرة دين الله، فجعله الله نورا يهتدى به على مر العصور

الى الذين قدموا أجسادهم قربانا للعراق، وصاروا شموعا تنير درب الحرية نحو بناء بلد يطمح أن يكون يوما معافى...

شهداؤنا الابرار

الى من تحمل عناء الحياة القاسية في سبيل أن يوصلنا الى درب النجاح، فكان خير سندٍ..

أبي الغالي

الى من تعلمت منها كل شي نافع، يضيئ درب المستقبل، يامن حملتني على أكف الراحة منذ صغري...

أمي الغالية

الى روح أخي عدي رَحمهُ الله.....

الإهداء

الى زوجتي الغالية التي هي خير عون لي....

الى كل العقول النيرة والاقلام النابضة بالحياة....

أهدي هذا الجهد المتواضع.....

ضرغام

شكر وتقدير

الحمد لله الذي ذكره شرف للذاكرين وشكره فوز للشاكرين وحمده عز للحامدين وطاعته نجاه للمطيعين. وأتم الصلاة وأفضل التسليم على محمد وآله الطاهرين.

وبعد: فعن رسول الله (ﷺ) أنه قال: من لم يشكر الناس لم يشكر الله. فبعد الانتهاء من هذه الدراسة يطيب لي في مقام الشكر أن أسجل إمتنان شكري وتقديري إلى الأستاذة الفاضلة الدكتورة إسراء محمد علي سالم المشرفة على هذه الرسالة فلولا شمولي برعايتها لما اهتديت إلى بر الأمان.

كما أتقدم بشكري وامتناني إلى الأساتذة الأفاضل في معهد العلمين للدراسات العليا لجهودهم الخيرة التي بذلوها خلال السنة التحضيرية.

وما دمت في مقام الشكر والعرفان فلا يسعني إلا أن أقدم شكري الجزيل إلى موظفي مكتبة كلية القانون - جامعة الكوفة وجامعة بابل وجامعة النهرين وأمناء المكتبتين في الروضة الحيدرية ومسجد الكوفة لتعاونهم معي في تسهيل مهمة حصولي على المصادر المتعلقة بالرسالة.

شكر وتقدير

وأخيراً فإني وإن ذكرت بعض الأسماء دون الأخرى فإن ذلك لايعني عدم الوفاء والتنكر للقسم الآخر بل لهم جميعاً - بعد المعذرة - شكري أكثر مما تحويه الأسطر وتقدمه الكلمات.

الباحث

المقدمة

الحمد لله رب العالمين الذي علم الانسان مالم يعلم، وأسبغ عليه نعمة ظاهرة وباطنة، فله الحمد في الأولى والآخرة على جميع نعمه، والصلاة والسلام على المبعوث رحمة للعالمين سيدنا محمد وآله الطاهرين.

أما بعد...

أن التجسس ظاهرة جرمية قديمة قدم البشرية، وأخذت هذة الظاهرة أشكالا مختلفة وأساليب متعددة ومورست لغايات متباينة، وكانت الى وقت قريب نسبيا مقتصرة على الأمور العسكرية والسياسية، إلا أنها أخذت تتسع في الوقت الحاضر لتشمل الجانب الاقتصادي والصناعي والعلمي...الخ، مما زاد من مخاطرها على أمن الدول ومؤسساتها العامة، والمؤسسات والشركات والمنظمات الخاصة وكذلك على الحياة الخاصة، وكان للوسائل التقنية دور كبير في تسهيل ارتكاب جريمة التجسس المعلوماتي، كما نجد أن جريمة التجسس قد مورست من قبل الدول رغم تشريعها لقوانين تجرمها، كما ترتكب من قبل الجماعات والأفراد.

وتأسيسا على ذلك أرتأيت أن تكون **(جريمة التجسس المعلوماتي / دراسة مقارنة)** موضوعا لهذة الدراسة.

أولا: أهمية الدراسة:

تعد جريمة التجسس المعلوماتي من الجرائم الخطيرة في الوقت الحاضر، فهي من الجرائم العابرة للحدود الوطنية والتي تهدد أمن الدول كما تهدد وجود الشركات أو المؤسسات التجارية والصناعية والاقتصادية والمالية والعلمية وتنتهك حرمة الحياة الخاصة، أذا أصبحت البيانات والمعلومات العلمية والمالية والتجارية...الخ، هي أساس نجاح وتطور هذة الدولة أو المؤسسة أو الشركة أو تلك، كما أن الاتصالات والصور والخرائط أضافة الى ما تقدم تعتبر سلع تستخدم للبيع والشراء والتهديد والابتزاز وغيرها من الأفعال غير المشروعة، كما يزيد من الأمر تعقيدا إذا ما عرفنا أن هذة الجريمة ترتكب من قبل الموظفين بالمؤسسسات أو الشركات...الخ، والذين عادة ما يقومون بدور أيجابي في أرتكاب جريمة التجسس، أو يكون لهم دورٌ سلبي بالوقوف موقف المتفرج، بدلاً من أداء دورهم في حفظ سرية وسلامة ما أئتمنوا عليه، وقد يكون الاختراق من قبل أشخاص من خارج المؤسسات يتمتعون بقدر من المعرفة التقنية، والذين عملت بعض الدول أو الشركات أو المؤسسات الى أستأجارهم ليعملوا لصالحها، ليقوموا بأختراق الحواجز الامنية للأنظمة المعلوماتية أو الشبكات المعلوماتية أو المواقع الالكترونية أو غيرها من الوسائل التقنية للحصول على البيانات أو المعلومات السرية.

وتعتبر جريمة التجسس من الجرائم ذات طبيعة متغيرة ترتبط طبيعتها مع النظام القانوني الذي يحكمها(أو الحق المعتدى عليه)، فقد تكون سياسية أذا انصبت على حقوق سياسية أو كان الدافع منها سياسيا، كما أنها تعد من جرائم أمن الدولة أذا كان أرتكابها يهدد أمن وسلامة الدولة كما في حالة الحصول على معلومات تخص قدرة أو أمكانيات القوات المسلحة مثلا، كما أنها تعد من الجرائم العادية في حال كان محلها أسرار الحياة الخاصة لأشخاص عاديين.

ثانيا: مشكلة البحث:

تتمحور مشكلة البحث في أن البيانات أو المعلومات السرية سواء تعلقت بالدولة أو الشركات أو المؤسسات أو الأفراد وغيرها، رغم تأكيد مختلف قوانين الدول والقانون الدولي والمعاهدات والمؤتمرات والشريعة الاسلامية، على ضرورة الحفاظ على هذة الأسرار أو البيانات أو المعلومات الا أنها دون جدوى، حيث لا تمنع من وقوع الاعتداء أيا كان صورته سواء كان بالدخول غير المشروع أو الاعتراض أو الالتقاط أو التنصت، للقيام بعد ذلك بالأفشاء أو الاذاعة أو النسخ أو النشر أو الاطلاع وغيرها، من أجل غايات متباينة قد تكون من أجل الكسب أو التهديد أو الابتزاز أو البيع أو الشراء، لذلك سيحاول البحث بيان المخاطر التي تهدد أمن البيانات، والوسائل أو الطرق أو البرامج التي تساعد على توفير الحماية، وبيان طبيعة جريمة التجسس المعلوماتي، وكذلك تحديد ماهية الافعال التي تشكل أعتداء على سرية البيانات أو المعلومات.

إن موضوع جريمة التجسس المعلوماتي من الموضوعات الشائكة والحساسة والحديثة في الوقت ذاته، حيث تثير العديد من الاشكالات على المستوى القانوني والقضائي، فعلى المستوى القانوني نحن محكومون بالشرعية الجزائية، أي لا جريمة ولا عقوبة الا بنص أو بناء على نص، مما يجعلنا عاجزين عن تطبيق النصوص القانونية في حال ظهور صورة جديدة للتجسس المعلوماتي والتي هي رهن ما يحصل من تطور، مما يستدعي التدخل المستمر من أجل تعديل النصوص القانونية، أما على المستوى القضائي فأن جريمة التجسس المعلوماتي من الجرائم العابرة للحدود الوطنية مما تثير مشاكل حول الولاية القضائية، علاوة على ذلك هل القواعد العامة لقانون العقوبات تنطبق على جريمة التجسس المعلوماتي ولا سيما في العراق مع وجود مشروع قانون الجرائم المعلوماتية لعام 2012 والذي لم يقر لحد الآن.

وعلى مستوى التطبيقات القضائية وجدنا ندرة القرارات القضائية بشأن جريمة التجسس المعلوماتي بصورة عامة على الرغم من أن الواقع العملي يأكد كثرة وقوعها في الوقت الحاضر وخاصة في العراق.

لكل ما تقدم نأمل أن تكون هذهِ الدراسة مساهمة متواضعة لرفد هذا الموضوع الحيوي بما نراه مفيدا من الأفكار العلمية للتوعية والوقاية من ظاهرة التجسس المعلوماتي ومكافحتها.

ثالثا: منهجية البحث:

إنَّ المنهج الأكثر انسجاما مع طبيعة الموضوع يقوم على الاستعانة بالمنهج النقدي والمنهج التحليلي فضلا عن المنهج المقارن، إذ أن عملية تفاعل المزايا الايجابية لهذهِ المناهج من شأنها أن تؤدي الى مستوى علمي متطور في أطار البحث العلمي يدعى التكامل المنهجي، وعمدنا الى جمع المعلومات المستخلصة من عموم المصادر وترتيبها وفق أطار علمي مستأنسين قدر الإمكان ببعض الأحكام القضائية.

رابعا: نطاق البحث:

يندرج موضوع **(جريمة التجسس المعلوماتي/ دراسة مقارنة)** ضمن أطار التشريعات الجنائية، لذلك فأن أساس البحث هو التشريع العراقي متمثلا بقانون العقوبات رقم 111 لسنة 1969 المعدل ومشروع قانون الجرائم المعلوماتية لعام 2012، والتشريعات الوطنية المقارنة الأجنبية والعربية الخاصة بمكافحة الجرائم المعلوماتية، وكيفية معالجتها لهذة الجريمة كالقانون الفرنسي لعام 1992 المعدل، وقانون مكافحة جرائم إساءة استخدام الحاسب الأمريكي لعام 1984 المعدل، ونظام مكافحة الجرائم المعلوماتية السعودي لعام 2007، ومرسوم مكافحة جرائم تقنية المعلومات الاماراتي لعام 2012، بيد أن طبيعة هذة الدراسة والمنهجية المتبعة فيها اقتضت تناول بعض الاتفاقيات والمواثيق والاعلانات والمؤتمرات الدولية.

خامسا: خطة البحث:

إنَّ طبيعة موضوع (جريمة التجسس المعلوماتي/ دراسة مقارنة) والغرض منه، تجعل من المناسب أن نتناوله في ثلاثة فصول تسبقهم مقدمة:

- **سنتناول في الفصل الأول** ماهية الجريمة المعلوماتية وذلك عبر مبحثين نبين في المبحث الأول مفهوم الجريمة المعلوماتية، أما المبحث الثاني فسنوضح فيه المخاطر التي تتعرض لها البيانات المعلوماتية وأمنها المعلوماتي.
- **أما الفصل الثاني** فسيخصص لماهية جريمة التجسس المعلوماتي، وذلك في مبحثين نفرد المبحث الأول لمفهوم جريمة التجسس المعلوماتي، ونكرس المبحث الثاني لطبيعة جريمة التجسس ونطاقها.
- **ونستعرض في الفصل الثالث** بعض صور جريمة التجسس المعلوماتي، من خلال مبحثين نفرد المبحث الأول لجريمة الدخول غير المشروع، ونكرس المبحث الثاني لجريمة الاعتراض أو الالتقاط أو التنصت المعلوماتي.

الفصل الأول

ماهية الجريمة المعلوماتية

في بداية الستينات والسبعينات من القرن الحادي والعشرين، ظهرت أول معالجة لما يسمى بجرام الكومبيوتر، واقتصرت هذه المعالجة على مقالات تناقش التلاعب بالبيانات المخزونة وتدمير أنظمة الكومبيوتر، والتجسس المعلوماتي، والاستخدام غير المشروع للبيانات المخزونة في نظم الكومبيوتر، وفيما اذا كانت تلك السلوكيات غير المشروعة، جرائم بالمعنى القانوني أم سلوكيات غير أخلاقية في بيئة الكترونية، وبقى التعامل مع هذه السلوكيات يميل الى النطاق الأخلاقي أكثر من النطاق القانوني[1]، مما دعى فقهاء القانون الجنائي إلى الاهتمام بدراسة جرائم التقنية المعلوماتية باعتبارها ظاهرة فرضت نفسها على المجتمع، لما تنطوي عليه هذه الجريمة من صفات خاصة حيث كان لصلتها بالحاسوب الآلي الصفة المميزة لها عن غيرها من الجرائم[2]. فقد شهدت زيادة في ارتكابها، نتيجة ازدياد العالم باستخدام الانترنت، كما تنوعت أساليب ارتكابها وتنوع محل الجريمة،

(1) د. خالد ممدوح إبراهيم، الجرائم المعلوماتية، ط1، دار الفكر الجامعي، الإسكندرية، 2009، ص71.

(2) د. علي جعفر، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة، ط1، منشورات زين الحقوقية، بيروت، 2013، ص75.

فمنها ما يمثل الاستغلال غير المشروع للبيانات المخزونة داخل الكومبيوتر، أو اختراق للكومبيوتر والاطلاع على الملفات السرية أو تدمير البرامج والبيانات بواسطة الفيروس وغير ذلك، بحيث أصبحت شبكة الأنترنت بؤرة اجرام مثالية تتعدى الأجهزة الأمنية والقضائية بثغرات قانونية ضخمة[1].

وتأسيسا على ما تقدم، سنتناول في هذا الفصل مفهوم الجريمة المعلوماتية، و المخاطر الألكترونية التي تتعرض لها البيانات و أمنها المعلوماتي، و ذلك من خلال مبحثين وعلى النحو الآتي.

(1) د. عماد مجدي عبد الملك، جرائم الكومبيوتر والانترنت، دار المطبوعات الجامعية، الإسكندرية، 2011، ص27 - 28.

المبحث الأول

مفهوم الجريمة المعلوماتية

سنبين في هذا المبحث، تعريف الجريمة المعلوماتية وسماتها وتصنيف مرتكبيها، وذلك في مطلبين:

- **يخصص المطلب الأول** لتعريف الجريمة المعلوماتية.
- **ونفرد المطلب الثاني** لسمات الجريمة المعلوماتية وتصنيف مرتكبها.

المطلب الأول

تعريف الجريمة المعلوماتية

- سنعرف الجريمة المعلوماتية لغة.
- ومن ثم اصطلاحا وذلك في فرعين.

الفرع الأول

تعريف الجريمة المعلوماتية لغة

الجريمة لغة:

الذنب، ومن اشتقاقاتها جَرمَ وأجرم واجترم، والجِرم بالكسر يعني الجسد، وتَجّرم عليه ادعى عليه ذنبا لم يفعله[1]، والجُرم هو الذنب أو الجناية[2].

أما المعلوماتية لغة:

من اشتقاقات الفعل عَلِمَ وعَلِم بالشيء[3] علما أي عَرفَه، و أعلم الشيء يعني جعل له علامة، وتعالم الجميع الشيء أي عرفوه، والمعلم يراد به ما يستدل به على الطريق من أثره [4].

وجاءت كلمة معلومات للدلالة على التوقيت في قوله تعالى ﴿الْحَجُّ أَشْهُرٌ مَّعْلُومَاتٌ﴾[5] وكذلك قوله تعالى: ﴿وَيَذْكُرُوا اسْمَ اللَّهِ فِي أَيَّامٍ مَّعْلُومَاتٍ﴾"[6]، وكلمة علم تعني أدرك الشيء بحقيقته[7].

(1) محمد بن عبد القادر الرازي، مختار الصحاح، مكتبة لبنان، بيروت، 1986، ص43.

(2) إبراهيم مصطفى وآخرون، المعجم الوسيط، ج1، ط 2، دار الدعوة، استانبول، 1989، ص 118.

(3) اسماعيل بن حماد الجوهري، الصحاح تاج اللغة وصحاح العربية، ج 1، دار الكتاب العربي، القاهرة، دون سنة نشر، ص 31.

(4) محمد بن عبد القادر الرازي، مختار الصحاح، دار الرسالة، الكويت، 1982، ص452.

(5) سورة البقرة، من الآية (197).

(6) سورة الحج، من الآية (28).

(7) إبراهيم مصطفى وآخرون، ج 2، ط 2، مرجع سابق، ص624.

وبالنسبة لمصطلح المعلوماتية في اللغة الانكليزية:

فيقابلها تعبير (Information) [1]، في حين تستخدم عبارة (connaissance) في اللغة الفرنسية[2].

(1) منير البعلبكي، المورد القريب قاموس أنكليزي – عربي، دار الزهراء، أيران، 2006، ص 208.

(2) نهاد الخطيب، قاموس الزاخر (عربي – فرنسي)، ط1، الزاخر، بيروت، 2011، ص 234.

الفرع الثاني

تعريف الجريمة المعلوماتية اصطلاحا

قانونا لم تعرف أغلب التشريعات محل الدراسة الجريمة المعلوماتية، ألا أن المشرع السعودي عرفها بأنها " أي فعل يرتكب متضمنا استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام " [(1)].

وبالنسبة للفقه فقد تعددت التعريفات للجريمة المعلوماتية بأبراز الوسيلة المرتكبة بها الجريمة، أو التركيز على موضوع الجريمة، أو التقنية المستخدمة، أو التركيز على جانبي الربح أو الخسارة لطرفي الجريمة المعلوماتية.

فقد عرفت بأنها: (كل أشكال السلوك غير المشروع أو الضار بالمجتمع الذي يرتكب باستخدام الحاسب) [(2)].

وأيضا (هي نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزونة داخل الكومبيوتر أو تلك التي يتم تحويلها عن طريقه)[(3)]، **وأيضا** (هي أية جريمة يكون ضروريا لارتكابها أن يتوافر لدى فاعلها معرفة بتقنية الحاسب)[(4)].

كما عرفت بأنها (هي الأفعال العمدية التي سببت خسارة للحكومة أو ربح للأفراد والمرتبطة بتصميم أو استخدام أو تشغيل النظام الذي تقع هذه الأفعال في

(1) ينظر: (الفقرة 8 من المادة 1) من نظام مكافحة الجريمة المعلوماتية السعودي رقم (17) لسنة 2007.

(2) د. رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن، ط1، منشورات الحلبي الحقوقية، بيروت، 2011، ص39.

(3) د. خالد ممدوح إبراهيم، الجريمة المعلوماتية، مرجع سابق، ص74.

(4) سامي علي حامد عياد، الجريمة المعلوماتية واجرام الانترنت، دار الفكر الجامعي، الاسكندرية، 2007، ص40.

نطاقة)[1]، من الملاحظ على التعريفات أنها تأكد على توافر المعرفة التقنية لدى الفاعل حتى يتمكن من أرتكابها أو اقترافها[2]، وهو شرط من وجهة نظري ليس ضروريا، إذا أن كثير من الهواة يقومون بأرتكاب الجريمة المعلوماتية، وهم لا تتوفر لديهم المعرفة الكافية بالتقنية المعلوماتية، فالمعرفة بالتقنية ليست شرطا لتحقق الجريمة، كما أنها تربط مسألة التجريم بالربح والخسارة مما يؤدي إلى افلات الكثير ممن يقومون باختراق النظام لمجرد اثبات البراعة والذكاء[3].

أما قضاءا فلم أجد تعريفا للجريمة المعلوماتية، حسب ما أطلعت عليه من مصادر، وقرارات قضائية.

ولكن يمكن إيراد تعريفاً لها حسبما ذكرته وزارة العدل الأمريكية في دليلها لعام 1979 بأنها (أي جريمة لفاعلها معرفة فنية بالحاسبات تمكنه من ارتكابها)[4].

من كل ما تقدم يمكن أن نضع تعريفا للجريمة المعلوماتية ونقول بأنها (كل تصرف غير مصرح به أو تجاوز التصريح الممنوح، يرتكب باستخدام تقنية المعلومات، يقع على الانظمة المعلوماتية أو المواقع الالكترونية أو الشبكات المعلوماتية أو أيا من الوسائل التقنية، يترتب عليه ضرر، سواء حقق الجاني مكسبا أم لا).

(1) سامي علي حامد عياد، مرجع نفسه، ص 42 - 43.

(2) جلال محمد الزغبي واسامة احمد المناعسة، جرائم تقنية نظم المعلومات الالكترونية، دار الثقافة، عمان، 2010، ص67.

(3) جلال محمد الزغبي واسامة احمد المناعسة، مرجع سابق، ص66.

(4) محروس نصار غايب، الجريمة المعلوماتية، مجلة التقني، المعهد التقني - محافظة الانبار، مجلد 24، العدد 9، 2011.

المطلب الثاني

سمات الجريمة المعلوماتية وتصنيف مرتكبيها

تمتاز الجريمة المعلوماتية بعدد من السمات التي تميزها عن غيرها من الجرائم التقليدية، كما أن مرتكبي هذه الجرائم ليسوا من صنف واحد.

وعليه سنحدد في هذا المطلب:

- سمات الجريمة المعلوماتية.
- وتصنيف مرتكبيها، وذلك في فرعين.

الفرع الأول

سمات الجريمة المعلوماتية

ارتباط الجريمة المعلوماتية بأجهزة الاتصالات المختلفة كالكومبيوتر والهاتف النقال وغيرها من أجهزة الاتصال وارتباط هذه الأجهزة بشبكة الأنترنت أضفى على الجريمة المعلوماتية سمات تميزها عن الجريمة التقليدية سواء بالسمات العامة للجريمة أو في الباعث على ارتكابها أو في طريقة تنفيذ الجريمة، وأهم هذه السمات هي:

أولا: الجريمة المعلوماتية جريمة عابرة للحدود:

إذ ان الجريمة المعلوماتية لا تعترف بالحدود الجغرافية، حيث ترتكب من مجتمع يستطيع من خلال شبكات الأنترنت، أن يخترق الزمان والمكان دون الخضوع لحرس الحدود[1]، وساعد في ذلك ربط أعداد هائلة من الحواسيب عبر العالم بهذه الشبكات، حيث يكون في أغلب الأحيان الجاني في بلد والمجني عليه في بلدٍ آخر[2]، أضافة إلى السرعة في ارتكاب الجريمة والتي يوفرها النظام المعلوماتي، فترتكب العديد من الجرائم مثل جرائم الاعتداء على قاعدة البيانات، أو تزوير أو اتلاف السندات الألكترونية، أو التجسس على الحكومات والشركات والأفراد، أو سرقة بطاقات الائتمان والقرصنة وغسيل الأموال وغيرها [3]، وتعتبر الجرائم التي ترتكب في طار التعاملات المالية هي الأكثر شيوعا، وخاصة بعد استخدام

(1) نهلاعبد القادر المومني، الجريمة المعلوماتية، ط 2، دار الثقافة، عمان، 2010، ص50.

(2) د. عماد مجدي عبد الملك، مرجع سابق، ص43.

(3) د. خالد ممدوح إبراهيم، الجرائم المعلوماتية، مرجع سابق، ص77.

شبكة الانترنت في المعاملات البنكية، وبصفة خاصة بالتحويل الالكتروني للأموال والتبادل الالكتروني للمعلومات[1].

فالفاعل يرتكب جريمته بالاعتداء على البيانات أو المعلومات وغيرها، وهو بعيدا عن مسرح الجريمة، يعزز ذلك عدم وجود حماية كافية تصد مثل هكذا انتهاك، تجعل من مستخدموا شبكات الانترنت يشعرون بالأمان، إذ أن الاعتداء على نظم المعالجة الآلية، تظهر بأنماط مختلفة من السلوك حيث يستطيع الجاني الدخول إلى نظم المعالجة الآلية في أي بلد، وإعداد برامج خبيثة مثل (الفيروس)، وإرسالها إلى مناطق مختلفة من العالم، مما أثارت هذه الطبيعة للسلوك الكثير من المشاكل ولا زالت تثير حول تحديد الدولة صاحبة الاختصاص القضائي، وهل أن القوانين التقليدية بإمكانها أن تحكم الجريمة المعلوماتية، وما هو الدور الدولي في مكافحة الجريمة[2].

ثانيا: صعوبة اكتشاف الجريمة المعلوماتية و اثباتها:

تعتبر هذه السمة من أهم السمات المميزة للجريمة المعلوماتية، والسبب يعود لعدم تركها آثارا مادية أو قولية أو حالات تلبس[3]، كما هو الحال في أغلب الجرائم التقليدية، إذا أن اكتشاف الجريمة المعلوماتية يكون بمحض الصدفة[4] وذلك لعدة أسباب منها، عدم وجود أثر كتابي إذ يتم نقل المعلومات بالنظام الألكتروني، علاوة على أن الجاني يستطيع تدمير الآثار التي تدينة مثل تدمير القرص الصلب[5]،

(1) د. نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، ط1، منشورات الحلبي الحقوقية، بيروت، 2005، ص52.

(2) د. رشيدة بوكر،مرجع سابق، ص100 - 101.

(3) د. عفيفي كامل عفيفي، جرائم الكومبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، منشأة المعارف، الاسكندرية، 2000، ص 469.

(4) محمود احمد عبابنة، جرائم الحاسب وأبعادها الدولية، دار الثقافة، عمان، 2005، ص 303 - 304.

(5) منى فتحي احمد عبد الكريم، الجريمة عبر الشبكة الدولية للمعلومات (internet) صورها =

كما أنها تحتاج إلى خبرة فنية يصعب على المحقق التقليدي التعامل معها، كما أنها تعتمد على الخداع في ارتكابها وعلى التضليل في التعرف على مرتكبها[1]، إذ يصعب التوصل إلى الجاني وتحديد هويته نظرا لدخوله الشبكة تحت اسم مستعار[2]، إذ يقوم الجاني بالأعمال غير المشروعة، من خلال الدخول إلى شبكة بعيدة عنه [3]. يضاف الى ذلك أن للمجني عليه دورا في تعزيز مجهولية الفاعل، كما تحرص الجهات التي تتعرض أنظمتها المعلوماتية للانتهاك، إلى عدم الكشف حتى بين موظفيها عما تتعرض له، باتخاذ إجراءات داخلية دون ابلاغ السلطات تجنبا للإضرار بسمعتها، بل هنالك من يرى ان المجني عليه، يسهم بصورة غير مباشرة في ارتكاب الفعل، وذلك بسبب وجوده في ظروف تجعل من امكانية تعرضه للاختراق كبيرة[4]، وهذا الظروف سوف يتم توضيحها عند الكلام عن كيفية اصابة الحواسيب بالفيروس أو الديدان وغيرها في المبحث الثاني من هذا الفصل.

إنَّ صعوبة كشف الجريمة المعلوماتية هي مسألة نسبية، فهنالك جرائم معلوماتية تم الكشف عنها في الولايات المتحدة الامريكية مثلا، حيث استطاع المحققون التوصل إلى الهكر الإسرائيلي الذي استطاع الوصول إلى معلومات حساسة داخل حواسيب في أمريكا وإسرائيل، ومن خلال التحقيق وجد أن مصدر الاختراق من داخل الكيان الصهيوني وبالتعاون مع جهات التحقيق الاسرائيلية، تم معرفة الفاعل وضبط كافة الأجهزة المستخدمة في عملية الاختراق[5]، وأيضا

= ومشاكل اثباتها، أطروحة دكتوراه، جامعة القاهرة كلية الحقوق، ص 140 - 141.

(1) د. عماد مجدي عبد الملك، مرجع سابق، ص 43 - 44.

(2) د. محمد محمود المكاوي، الجوانب الأخلاقية والاجتماعية والمهنية للحماية من الجرائم المعلوماتية (جرائم الكومبيوتر والانترنت) المكتبة العصرية، القاهرة، 2010، ص34.

(3) محمود احمد عبابنة، مرجع سابق، ص37.

(4) نهلا عبد القادر المومني، الجرائم المعلوماتية، ط2، دار الثقافة، عمان، 2010، ص 54 - 55.

(5) د. يوسف حسن يوسف، الجرائم الدولية للانترنت، ط 1، المركز القومي للاصدارات القانونية، القاهرة، 2011، ص 53.

استطاعت السلطات الألمانية من التوصل إلى مرتكب جريمة الغش المعلوماتي من خلال وجود اتصال بين جهاز الكومبيوتر في المانيا وبين شبكة اتصال في سويسرا حيث تم ضبط البيانات المخترقة داخل حاسب الجاني وكان ذلك بالتعاون مع السلطات في سويسرا [1].

وفيما يتعلق باثبات الجريمة فالمسألة نسبية أيضا، إذ بالإمكان استخدام التقنيات في أثبات الجريمة المعلوماتية ومن هذه التقنيات تقنية الاسترجاع، وهي تقنية تستخدم للحصول على المعلومات الموجودة في نظام معلوماتي، أو قريبة من نظام معلوماتي بعد تنفيذ عمل ما، إذ لا تستطيع بعض أنظمة التشغيل من محو الذاكرة المغلقة المستخدمة بواسطة الذاكرة المؤقته لمعطيات الأدخال والإخراج، وهنالك بعض أنظمة التشغيل لا تمحو مضمون ذاكرة الأسطوانة أو الشريط المغنط، لأن عملية المحو تتطلب وقتا طويلا، لذا يتم كتابة المعطيات الجديدة فوق المعطيات القديمة ومن ثم يمكن الحصول على المعطيات القديمة، قبل كتابة المعطيات الجديدة[2]، كما توجد برامج أخرى تستخدم للوصول إلى الملفات على الشبكة أو على القرص الصلب ونسخها قبل تدميرها من المتهم، وكذلك يوجد برنامج يتم من خلاله الحصول على محتويات القرص الصلب مهما كانت طريقة مسح البرامج أو المعلومات الموجودة عليه، بل هنالك برامج تستطيع معرفة المواقع التي تمت زيارتها قبل ستة أشهر وكذلك معرفة محتويات القرص الصلب حتى في حالة كسره أو تدميرِه جزئيا [3]، كذلك يمكن استخدام هواتف المطلوبين قضائيا

(1) د. خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، ط 1، دار الفكر الجامعي، الاسكندرية، 2009، ص 206.

(2) للمزيد: د. عمر أبو الفتوح عبد العظيم الحمامي، الحماية الجنائية للمعلومات المسجلة الكترونيا، دار النهضة العربية، القاهرة، 236. عبد العال الديربي ومحمد صادق إسماعيل، الجرائم الالكترونية دراسة قضائية قانونية مقارنة، ط1، المركز القومي للاصدارات القانونية، القاهرة، 2012، ص76.

(3) للمزيد من التفاصيل عن هذة البرامج ينظر: د. حسن طاهر داوود، جرائم نظم المعلومات، =

كأداة للتجسس عليهم، من خلال تشغيل الميكروفون أو الكاميرا للهواتف التي يحملوها ومعرفة تحركاتهم حتى وأن كان الجهاز في وضع الاغلاق[1].

ثالثا: المساهمة في أرتكابها:

إذ تتم الجريمة المعلوماتية من شخص لديه معرفة فنية في مجال الحاسوب، والذي يكون له دورٌ إيجابيٌ في المشروع الاجرامي، فمثلا يقوم الشخص المتخصص في تقنيات الحاسوب والانترنت بالجانب الفني من المشروع الاجرامي، وبالتعاون مع شخص من محيط المؤسسة المجني عليها أو من خارجها لتغطية عملية التلاعب وتحويل المكاسب إليه[2].

فعلى صعيد عمل المصارف يقوم موظف البنك، بتزويد العصابات الاجرامية بالبيانات الخاصة ببطاقة الائتمان الصحيحة والمتداولة، وذلك لغرض مساعدتهم في تقليد أو اصطناع هذه البطاقات، وبالتالي تتحقق الجريمة بأصطناع أو تقليد بطاقات ائتمان مزورة [3]، فالاشتراك بالجريمة المعلوماتية قد يكون إيجابيا وهو الغالب ويكون بتقديم مساعدة فنيه أو مادية، وقد يكون الاشتراك سلبيا يتمثل بعدم الإبلاغ من جانب من علم بوقوع الجريمة محاولة منه تسهيل اتمامها[4].

= جامعة نايف العربية للعلوم الامنية، الرياض، 2000، ص 299 - 230. د.عبد العال= =الديربي و محمد صادق اسماعيل، مصدر سابق، ص103 - 104. أحمد بن زايد جوهر حسن المهندي، تفتيش الحاسب الآلي وضمانات المتهم، رسالة ماجستير، أكاديمية شرطة دبي، دبي، 2009، 218 وما بعدها.

(1) للمزيد: عادل عزام سقف الحيط، جرائم الذم والقدح والتحقير المرتكبة عبر الوسائط الالكترونية، ط1، دار الثقافة، عمان، 2011، ص166.

(2) د.عادل يوسف الشكري، الجريمة المعلوماتية وأزمة الشرعية الجزائية، مركز دراسات الكوفة، العدد 7، 2008، ص 115.

(3) د. إيهاب فوزي السقا، الحماية الجنائية والأمنية لبطاقات الائتمان، دار الجامعة الجديدة، الإسكندرية، 2007، ص 201.

(4) نهلا عبد القادر المومني، مرجع سابق، ص58.

رابعا: اتساع نطاق الجريمة المعلوماتية:

شكلت الجريمة المعلوماتية غزوا لكل نواحي الحياة ومجالاتها المختلفة العسكرية منها والسياسية والاقتصادية والصناعية والاجتماعية وغيرها، ورغم ذلك فأن الدول تسير نحو إدخال الحاسب الآلي في مختلف الأنشطة والقطاعات الحكومية والخاصة[1]، ففي المجال العسكري تكون أسرار الدولة والمشروعات النووية والتصنيع الحديث للأسلحة، هو محل الجريمة المعلوماتية[2].

ومن الناحية الاقتصادية تمس الجرائم المعلوماتية المركز الحسابي والإداري والاستثمارات وتنقلات الأموال سواء في المنشأت العامة أو الخاصة[3]، كأن يقوم بعض الأشخاص بشراء كومبيوتر صغير جدا، ويقوم هذا الكومبيوتر بنسخ البيانات الموجودة على الشريط الممغنط حيث يتم الحصول على خصائص الهوية الالكترونية من القطاعات الممغنطة من إحدى البطاقات الصحيحة ثم يتم نقلها إلى بطاقات أخرى، وذلك بوضع شريط تسجيل الكتروني على البطاقة الأصلية وإمرار تيار حراري ثم يوضع على شريط البطاقة الأصلية شريط ممغنط فارغ للبطاقة المراد نقل البيانات إليها ويمرر أيضا تيار حراري حيث يتم نسخ البيانات[4].

أما على الصعيد التجاري والصناعي، حيث تنصب الجرائم المعلوماتية على الدراسات الخاصة بالتصنيع والإنتاج والتجارة والاستثمار والقطاع الصناعي للإنتاج ومراكز البيع والتوزيع[5].

---

(1) د. عمر أبو الفتوح عبد العظيم الحمامي، مرجع سابق، ص 140.

(2) د. محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، ط1، دار النهضة العربية، القاهرة، 2003، ص69.

(3) د. عمر أبو الفتوح عبد العظيم الحمامي، مرجع سابق، ص142.

(4) د. إيهاب فوزي السقا، مرجع سابق، ص 188 - 189.

(5) د. محمد سامي الشوا، مرجع سابق، ص 68.

كما وتستهدف هذه الجرائم أيضا المعلومات الشخصية، من خلال اختراق البريد الألكتروني والاعتداء على الملكية الفكرية وعلى الأشخاص بالسب والاهانه والاطلاع على الصور الشخصية وكل ما يحتويه الحاسب الشخصي، كما تستهدف البيانات الشخصية المخزونة في ذاكرة حواسيب البنوك وشركات التأمين والمستشفيات والأحزاب ومراكز الشرطة[1].

يضاف الى ما تقدم أنّ العمل السياسي هو كذلك محل لهذة الجرائم، ومن صورها الاعتداء على حرية التعبير، حيث تفرض بعض الدول رقابة على شبكة الانترنت، إذ تملك مزود واحد لخدمات الانترنت يخضع لرقابة الحكومة وتقوم بأعتقال المدونين وبشكل خاص المعارضين السياسيين عندما يقوموا بتناول الحكومة بالنقد والتحريض[2].

خامسا: وقوع الجريمة المعلوماتية في احدى المراحل الاساسية لعملية تنظيم البيانات

ترتكب الجريمة المعلوماتية اثناء المعالجة الآلية للبيانات[3] والمعطيات الخاصة بالكومبيوتر، فنشاط الجاني في الجريمة المعلوماتية يتمثل بالتعدي على نظام معالجة البيانات[4] اذ تقع الجريمة المعلوماتية في إحدى المراحل الأساسية لعملية المعالجة الآلية للبيانات فهي ترتكب في مرحلة ادخال البيانات، أو أثناء مرحلة المعالجة، أو أثناء مرحلة إخراج المعلومات، غير أنّ لكل مرحلة من هذه

(1) د. عادل يوسف الشكري، مرجع سابق، ص 116.

(2) عادل عزام سقف الحيط، مرجع سابق، ص175.

(3) المعالجة الآلية للبيانات يقصد بها: (العمليات والمهام التي تخضع لبيانات الحاسوب بما في ذلك إنشاؤها أو أرسالها أو أستقبالها أو تخزينها أو تجهيزها بأي وجه آخر). ينظر: الفقرة ثانيا من المادة 1) من مشروع قانون الجرائم المعلوماتية العراقي لعام 2012.

(4) د. خالد ممدوح إبراهيم، الجرائم المعلوماتية، مرجع سابق، ص 84.

المراحل نوعية خاصة من الجرائم وإنَّ الوقت الأمثل لأرتكابها هو مرحلة التشغيل[1]، إذ هي مرحلة الادخال وفيها تترجم المعلومات إلى لغة مفهومة من قبل الآلة، أذ يسهل ادخال معلومات غير صحيحة أو عدم إدخال البيانات المطلوبة أساسا، وهي مرحلة يتم فيها ارتكاب أكثر الجرائم المعلوماتية، أما مرحلة المعالجة يتم فيها تشغيل برامج جديدة تلغى جزئيا أو كليا عمل البرامج الأصلية أو استبدال البيانات الأصلية بيانات غير مطلوبة[2]، أما المرحلة المتعلقة بأخراج البيانات وفيها يتم التلاعب في النتائج التي يخرجها النظام المعلوماتي، بشأن بيانات أدخلت فيه وتمت معالجتها بطريقة صحيحة[3].

(1) د. عادل يوسف الشكري، مرجع سابق، ص115.

(2) د. حاتم عبد الرحمن منصور الشحات، الجرائم المعلوماتية، ط1، دار النهضة العربية، القاهرة، 2003، 237 وما بعدها.

(3) د. خالد ممدوح إبراهيم، التقاضي الالكتروني الدعوى الالكترونية وأجراءاتها أمام المحاكم، ط1، دار الفكر الجامعي، الاسكندرية، 2007، ص 329.

الفرع الثاني

تصنيف مرتكبي الجريمة المعلوماتية

إنَّ مرتكبي الجرائم المعلوماتية - كما سبق القول - ليسوا على درجة واحدة من الكفاءة والخطورة، حيث يتم تصنيفهم بحسب امكانيتهم أو مقصدهم من ارتكاب الجريمة المعلوماتية، حيث تمتاز أفعالهم عن أفعال المجرم التقليدي بسرعة وسهولة التنفيذ وإمكانية محو الآثار الجرمية، وهم كما يلي.

أولا: القراصنة:

القراصنه هم مبرمجون على مستوى عالٍ، يستطيعون اختراق حاسوب معين والاطلاع على محتوياته بواسطة برامج مخصصة للاختراق، ومن ثم يتم اقتحام الأجهزة المرتبطة معه وترتكب عمليات القرصنة عبر شبكة الانترنت غالبا سواء كانت هذه الشبكة يرتبط بها عدة حواسيب حول العالم او شبكة داخلية[1].

وتسهم قرصنة البرامج بشكل كبير في انتشار الفيروسات وهو ما يعني تدمير للنظم المعلوماتية او الاعتداء على الخصوصية، والذي ينتج عنه خسائر مادية بشكل مباشر او غير مباشر، ناهيك عما تسببه من ارتفاع في أسعار البرامج الاصلية لتعويض الخسائر الناتجة عن عمليات القرصنة إضافة إلى الأموال الكثيرة التي تنفق من اجل حماية البرامج من عمليات القرصنة [2].

(1) د. عماد مجدي عبد الملك، مرجع سابق، ص84.

(2) د. حسن الفاخري ومحمد الالفي، جرائم الانترنت بين الشريعة الإسلامية والقانون، دار النهضة العربية، القاهرة، 2008، ص 161.

إن القراصنة في عالم الحاسب الآلي والشبكة الدولية على نوعين الهاكرز والكراكر.

فالهاكرز هو المتلصص الذي يقتحم حواسيب الغير، ويتاجر بالمعلومات، واذا ما واجهته أيا من برامج الحماية فأنه لا يستطيع تخطيها[1]. إذ يقومون بالتخريب المباشر والفوري الأثر، كمسح البيانات من جهاز الكومبيوتر أو تعطيل التطبيقات على الشبكة أو تعديل البرامج أو تحريف البيانات أو تزوير المعاملات ويدفعهم إلى ذلك الحقد على الآخرين أو الكسب المادي[2].

أما الكراكر يتميز عن الهاكرز بقدرته على اختراق نظم الحماية الموجودة حول الشبكات وأجهزة الحاسب الآلي والوصول إلى البرامج والبيانات[3]. فالهاكرز يقف عند برامج الحماية اما الكراكر فهو اكثر خطورة لقدرته على اختراق نظم الحماية يساعدهم في ذلك برامج الاختراق الموجودة على شبكة الانترنت والتي تقدم بالمجان او مقابل أسعار زهيدة، ومن ثم يذهب كل ما انفق في سبيل حماية الشبكات والحواسيب ادراج الرياح[4].

ثانيا: الموظفون (المخربون المهنيون):

إن الموظفين العاملين في المؤسسات والشركات هم على قدر كبير من الخطورة، لما يتمتعون به من معرفة في مجال الحاسوب، وعلمهم بأمور وخفايا دوائرهم من جهة وثقة المؤسسة بهم من جهة أخرى[5] وهؤلاء الموظفون على انواع عديدة منهم.

---

(1) منى فتحي احمد عبد الكريم، مرجع سابق، ص 26.

(2) د. عبد الفتاح بيومي حجازي، جرائم الكومبيوتر والانترنت في التشريعات العربية، ط1، دار النهضة العربية، القاهرة، 2009. ص 112.

(3) منى فتحي احمد عبد الكريم، مرجع سابق، ص 26.

(4) د. يوسف حسن يوسف، مرجع سابق، ص 129.

(5) د. خالد ممدوح أبراهيم، الجرائم المعلوماتية، مرجع سابق، ص 140 وما بعدها. محمد محمود المكاوي، مرجع سابق، 308.

الموظفون الساخطون و هم الذين يعبرون عن سخطهم تجاه منشأتهم من خلال تخريب جهاز الكومبيوتر أو اتلافه أو سرقته[1]، إذ يجدون متعة في الانتقام من منشأتهم ويسببون عادة خسائر فادحة[2] كونهم على علم بعمل مؤسساتهم وتعاملاتها، ايضا الموظفون الذين يجدون متعة في اختراق نظم الحاسوب هذه الفئة من الموظفون يقومون بأظهار ما لديهم من خبرات بهدف تحدي خبراء مصممي البرامج، وهم في الغالب مبرمجون أصلا، وتكون الخسائر الناتجة عنهم قليلة، وهم في مصاف محترفي الجرائم المعلوماتية، وأخيرا الموظفون الذين يعانون من مشاكل خاصة هذه الفئة من الموظفين المدمنين أو المقامرين...الخ والذين يقومون بارتكاب الجرائم المعلوماتية داخل منشأتهم لحسابهم أو لحساب الغير وتكون الخسائر عادة ضخمة خاصة اذا كانوا على مستوى عالٍ من التنظيم[3].

ثالثا: صغار نوابغ المعلوماتية:

صغار نوابغ المعلوماتية هم شباب لديهم ولع بالمعلوماتية والحاسبات الآلية يعملون على انتهاك ذاكرة الحواسب الآلية للقيام بأعمال غير مشروعة، داخل حواسيب المنشأت والشركات التجارية، وهؤلاء الشباب لا يقدرون مطلقا النتائج المحتملة لأعمالهم الاجرامية، حيث يدفعهم إلى ارتكابها ميولهم إلى المغامرة والتحدي والرغبة في الاكتشاف[4] مستخدمين في ارتكاب جرائمهم حواسيبهم الخاصة أو حواسب مدارسهم وتمتد أفعالهم إلى آلاف الكيلومترات عن مواقعهم الجغرافية، والغالب في هذه الفئة من مخترقي الحواسيب هم أغلبهم حسن النية،

(1) حمزة بن عفون، السلوك الاجرامي للمجرم المعلوماتي، رسالة ماجستير، جامعة الحاج لخضر باتنة، ليبيا، 2012، ص 43. د. يوسف حسن يوسف، مرجع سابق، ص 72.

(2) د. عمر أبو الفتوح عبد العظيم الحمامي، مرجع سابق، ص 90. سامي علي حامد عياد، مرجع سابق، ص95.

(3) د. عمر أبو الفتوح عبد العظيم المحامي، مرجع سابق، ص 86 وما بعدها.

(4) سامي علي حامد عياد، مرجع سابق، ص 52 وما بعدها.

فهم يبرزون نقاط الضعف بالنظام دون الحاق الضرر بالغير[1]، ونتيجه لذلك ظهر اتجاه بالفقه يرى بعدم اسباغ الصفة الجرمية على أفعال هذة الفئة[2].

رابعا: عصابات الجريمة المنظمة:

يمارس الجرم المنظم مجموعة من الأفراد على درجة عالية من التنظيم تتضمن مستويات من القيادة، تستخدم كل الوسائل لتحقيق مشروعها الاجرامي من عنف وتهديد وابتزاز ورشوة، ويشارك بالجرم المنظم رجال السياسة وأصحاب المناصب الرفيعة، لذلك أطلق عليها جرائم ذوي الياقات البيض[3] إذ تمارس هذه الجماعات مختلف أنواع الاجرام وأزداد الأمر سهولة عليهم في ارتكاب الجرائم عند ظهور العالم الرقمي، فهي تمارس مثلا عمليات سرقة السيارات واستخدام شبكة الانترنت لمعرفة في أي ولاية قطع السيارة المسروقة تكون غالية الثمن ومن ثم يقومون ببيعها[4] أو قرصنة السجلات الخاصة[5]، كما وتستغل هذه العصابات شبكة الانترنت وبالأخص مواقع التواصل الاجتماعي، لأرتكاب جرائم الاتجار بالبشر وذلك باغراء فتيات الأُسر الفقيرة ودفعهن للسفر إلى أمريكا أو أوروبا لغرض الزواج أو العمل، ومن ثم يقومون بالمتاجرة باعضائهن أو اخضاعهن للدعارة القسرية[6]، كما وجدت هذه الجماعات في شبكة الانترنت وسيلة لا تضاهى للقيام

(1) د. عبد الفتاح بيومي حجازي، مكافحة جرائم الكومبيوتر والانترنت في القانون العربي النموذجي، ط1، دار الفكر الجامعي، الإسكندرية، 2006، ص 91. د. عمر أبو الفتوح عبد العظيم المحامي، مرجع سابق، ص 85.

(2) د. محمد فاروق عبد الرؤوف الخن، جريمة الاحتيال عبر الانترنت، ط 1، منشورات زين الحقوقية، بيروت، 2011، ص 188.

(3) نهلا عبد القادر المومني، مرجع سابق، ص 87.

(4) د. يوسف حسن يوسف، مرجع سابق، ص 72.

(5) International Journal of Cyber Crime. Volume 8 Issue 1 January. June 2014. Page 7..

(6) عادل عزام سقف الحيط، مرجع سابق، ص 164.

بعمليات غسيل الأموال على نطاق أوسع حيث تدعم عمليات غسيل الأموال انشطة عصابات الجريمة المنظمة في تجارة المخدرات وتجارة الرقيق الأبيض[1].

خامسا: الجواسيس:

الجواسيس هم الاشخاص الذين يهدفون إلى جمع المعلومات لمصلحة دولهم، أو لمصلحة بعض الأشخاص، أو الشركات التي تتنافس فيما بينها[2]، مما دفع الدول والشركات والأفراد للعمل جاهدا للمحافظة على بياناتها من عمليات التجسس، وهي بذات الوقت تقوم بأعمال التجسس على بعضها البعض، حيث يقوم الجواسيس بسرقة الاسرار السياسية والعسكرية والاقتصادية، والتنصت على الهواتف النقالة الخاصة بالافراد وغيرها من عمليات التجسس[3]، اذ عمدت الدول منذ زمن بعيد إلى التجسس على الدول الأخرى العدوة منها والصديقة، من أجل تجنب مخاطر هذه الدول، والتفوق عليها وكان التجسس يرتكز في ذلك الوقت على الجانب العسكري فقط أما في الوقت الحاضر اتسع ليشمل الجانب الاقتصادي والتكنولوجي[4].

سادسا: أصحاب الآراء المتطرفة:

أصحاب الآراء المتطرفة هم أشخاص يقومون بنشر معتقداتهم وأفكارهم الوثنية والاجتماعية والسياسية عبر الانترنت[5] متعدين في ذلك كل الحدود

(1) نهلا عبد القادر المومني، مصدر سابق، ص 88.

(2) د. سليمان احمد فضل، المواجهة التشريعية والامنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية (الانترنت)، دار النهضة العربية، القاهرة، 2007، ص 23.

(3) د. عبد الفتاح بيومي حجازي، جرائم الكومبيوتر والانترنت في التشريعات العربية، ط1، دار النهضة العربية، القاهرة، 2009، ص 113 - 114.

(4) د. عمر أبو الفتوح عبد العظيم الحمامي، مرجع سابق، ص 104.

(5) د. إيهاب فوزي السقا، مرجع سابق، ص 137.

المعقولة والمعتدلة للحوار والنقاش مستهدفين تحقيق غايات أو قضايا ليست لها علاقة بمصالحهم الشخصية ويلجئون في سبيل تحقيق ما يعتقدونه إلى ارتكاب الأنشطة الاجرامية التي تلحق الضرر بالافراد والمجتمع والقطاعات الأخرى، بغية اصلاح المجتمع حسب وجهة نظرهم، وقد أدى هذا التطرف الفكري إلى ما يعرف بصراع الحضارات، حيث عمد المتطرفون إلى زج الدين في صراعاتهم وادعى بعضهم بأفضلية بعض الأديان في تحقيق التقدم الحضاري[1].

(1) د. عمر أبو الفتوح عبد العظيم الحمامي، مرجع سابق، ص 99 وما بعدها.

المبحث الثاني

المخاطر التي تتعرض لها البيانات والامن المعلوماتي

تتعرض البيانات المحفوظة داخل الحواسيب إلى مخاطر، وتنقسم هذه المخاطر إلى مخاطر الكترونية مثل برامج الفيروس والديدان الالكترونية وحصان طروادة وبرامج التجسس وغيرها، وإلى مخاطر طبيعية مثل الزلازل والفيضانات... الخ، وإلى مخاطر عامة مثل انقطاع التيار الكهربائي ودخول اشخاص من خارج المؤسسات إلى النظام المعلوماتي...الخ، وإلى مخاطر خاصة مثل اخطاء المستخدمين...الخ. وللتصدي الى هذة المخاطر عملت الدول إلى إيجاد الوسائل التي تواجه هذا الخطر فظهرت النظم التقليدية في تأمين البيانات، والنظم التقنية الحديثة في تأمينها[1].

وتأسيسا على ماتقدم سنستعرض تلك المخاطر التي تتعرض لها البيانات ثم نعرج بعد ذلك إلى الأمن المعلوماتي و ذلك من خلال مطلبين وعلى النحو الآتي.

(1) حازم نعيم الصمادي، المسؤلية في العمليات المصرفية الالكترونية، ط 1، دار وائل للنشر، عمان، 2003، ص 119 ومابعدها. د. خالد ممدوح أبراهيم، الجرائم المعلوماتية، مرجع سابق، ص 147.

المطلب الاول

المخاطر التي تتعرض لها البيانات

نظرا لتنوع المخاطر التي تتعرض إليها البيانات.

- سوف نتناول المخاطر الالكترونية والمخاطر الطبيعية التي تتعرض إليها البيانات.
- ثم نعرج لبيان المخاطر العامة والمخاطر الخاصة التي تتعرض لها، وذلك في فرعين وعلى النحو الاتي.

الفرع الاول

المخاطر الالكترونية و المخاطر الطبيعية

اولا: المخاطر الالكترونية:

يعتقد البعض أن عدم عمل جهاز الكومبيوتر بشكل صحيح بأن الذي اصابه هو فايروس، إلا أن هذا الكلام غير دقيق إذ إن ما يصيب الكومبيوتر قد يكون فايروسا او حصان طروادة او ديدان الكترونية...الخ من البرامج الضارة، فهي برامج وإن كانت كلها ميكروسكوبية، إلا أنها تختلف في انتقالها وفي تأثيرها وكيفية التخلص منها. وتجدر الاشارة إلى أنه ليست كل البرامج المتطفلة ضارة بل يوجد منها نافعة تستخدمها بعض الشركات في حماية حقوق التأليف ومحاربة الاستنساخ الغير قانوني، وتدخل كذلك في الاغراض العسكرية [1]، كما يمكن تطوير بعض البرامج الفيروسية لتقوم بعمل مضاد ضد الفيروسات إلا أن الامر يتطلب معرفة دقيقة بتركيب الفايروس الضار، وكذلك يمكن تطوير فيروسات تعمل على تشخيص اي تغير في البرامج المحملة في النظام ويقوم هذا الفيروس بفحص المجموعة (الاختبارية) [2]. وأن ظهور البرامج المتطفلة الضارة يرجع تقريبا الى بداية وجود الحاسوب في ستينات القرن الماضي، والذي اثار مخاوف لدى مستخدمي الحاسوب وكان دافعا في نفس الوقت الى تطوير برامج لمكافحة الفيروسات.

(1) د. مصطفى محمد موسى، السيرة الذاتية للفيروسات الالكترونية بين الوقاية والمكافحة والعلاج، ط1، دار الكتب القانونية، القاهرة، 2008، ص35.

(2) خالد ابو الفتوح فضالة، مدخل الى فيروسات الحاسب، ط4، دار الكتب العالمية، القاهرة، 1997، ص 151.

1. الفيروسات:

تعرف بأنها (برنامج مكتوب بإحدى لغات البرمجة بطريقة خاصة، قادر على تكرار نسخ نفسه وله قدرة على التحكم بالبرامج الاخرى[1]، أو هو عبارة عن برنامج للحاسب الالي يهدف إلى أحداث ضرر في نظام الحاسوب الالكتروني وله القدرة على ربط نفسه بالبرامج الأخرى، وله القدرة على التكاثر، إذ أنه يتولد ذاتيا ويقوم بالانتشار داخل برامج الحاسوب ومواقع مختلفة من الذاكرة) [2].

كما تستطيع البرامج الفايروسية تعديل البرامج الغير مرتبطة بها بواسطة ادخال هيكل برمجته داخل البرامج الاخرى المستهدفة، ويقوم بتنفيذ وتعديل عدد من البرامج ومنع إجراء أي تعديلات إضافية على هذه البرامج من الغير، وادراك التعديلات التي اجريت على برنامج ما. ونستطيع القول إذ لم يكن لبرنامج الفيروس هذا التأثير والقدرة فهو ليس فيروسا وانما شيئا آخر[3].

ومن الجدير بالذكر أن البعض يعتقد ان الملفات المحمية من الكتابة عليها لا يصيبها الفيروس، في حين أن للفيروسات إمكانية تغيير خاصية الملفات التي تم تحديدها على أنها للقراءة فقط ومن ثم الدخول إلى هذه الملفات، كما أن برنامج الفيروس يبحث دائما عن الملفات التنفيذية، فعن طريق تنفيذ هذه البرامج يستطيع الفيروس الانتشار، كما يصيب الفيروس البرامج التي لا تنفذ مباشرة عن طريق المستخدم والتي تحوي شفرة الفيروس، أما الملفات غير التنفيذية فهي لا يصيبها الفيروس الألكتروني على الاطلاق مثل الملفات الرسومية، والملفات النصية ذات الامتداد(Ini.Txt.Dat) وغيرها[4].

(1) خالد ابو الفتوح فضالة، مرجع نفسه، ص 39.

(2) د. عبد الفتاح بيومي حجازي، الجرائم المستحدثة في نطاق تكنلوجيا الاتصالات الحديثة، ط 1، دار الفكر الجامعي، الاسكندرية، 2009، ص505.

(3) د. مصطفى محمد موسى، السيرة الذاتية....، مرجع سابق، ص54.

(4) د. مصطفى محمد موسى، السيرة الذاتية....، مرجع نفسه، ص 56 - 57.

وللبرامج الفيروسية خصائص أهمها، آلية التكرار وهو الجزء الذي من خلاله الفيروس ينسخ نفسه، وآلية التخفي وهو الجزء الذي يقوم بإخفاء الفيروس عن الاكتشاف ويمكن أن يتضمن تشفير للفيروسات لمنع برامج مكافحة الفيروس من اكتشافه[1]، وآلية التنشيط وهو الجزء الذي يسمح للفيروسات بالانتشار، حيث يبحث الفيروس عن شروط معينة لينشط وينتقل إلى مرحلة التنفيذ، ويسمى هذا الجزء جذب الزناد، وآلية التنفيذ هو الجزء المسؤول عن عمل الفيروس بعد تنشيطه ويكون بشكل رسالة أو مسح ملفات[2].

كما أن هنالك أنواع عديدة من الفيروسات الألكترونية حيث قسمت في القرن العشرين الى فيروسات عامة العدوى وأخرى محدودة العدوى، وفيروس التحميل وفيروس النظام، وفيروسات المهاجمة لبرامج التشغيل وفيروسات مهاجمة لنظام التشغيل، وفي القرن الحادي والعشرون ظهرت تقسيمات أخرى وهي فيروسات قطاع التشغيل وفيروسات الملفات وفيروسات خفية وفيروسات متحولة وغيرها، وفيروسات المكان المستهدف داخل الكومبيوتر وتقسم الى فيروسات قطاع الاقلاع[3]، و فيروسات الميكرو، و فيروسات الملفات[4]، وهناك فيروس حسب المنشأ وتقسم إلى فيروس ذات منشأ شخصي وهي التي يقوم بأنشائها محترفي الألكترون الرقمي بهدف التخريب أو اللهو، وفيروسات ذات منشأ مؤسساتي تنتج هذه الفيروسات من قبل المؤسسات للتجسس على أفراد معينين أو استخدامها في الدراسات الاستخباراتية، وفيروس ذات منشأ برمجي وهو الفيروس الذي يكون نتيجة خطأ برمجي أو خطأ اثناء العمل، وفيروس حسب التأثير فيروسات حميدة

(1) د. خالد ممدوح ابراهيم، فن التحقيق...، مرجع سابق، ص427.

(2) خالد ابو الفتوح فضالة، مرجع سابق، ص51.

(3) منير محمد الجهني و ممدوح محمد الجهني، أمن المعلومات الالكترونية، ط1، دار الفكر الجامعي، الاسكندرية، 2005، ص51.

(4) د. محمد محمود مكاوي، مرجع سابق، ص129.

لا تأثير لها على أداء جهاز الحاسوب، ويكون عملها بفتح ثغرة في الجهاز للتنصت عليه، و فيروسات تقوم بتخريب مكونات الحاسب المادية [1] أو الصلبة وهو التغير الحاصل في برنامج التحميل الموجود في الذاكرة الدائمة (الرام) والذي يمثل التعديلات في المكونات الصلبة [2].

أما عن كيفية حصول العدوى بالفيروس، فله طرق عديدة منها وصول الفيروس بشكل رسالة الكترونية آمنة ويقوم الفيروس بعد فتحه بأعمال مدمرة مثل نسخ وتعديل الملفات[3]، كما يتنقل الفيروس من حاسب إلى آخر من خلال الملفات المصابة او عن طريق الملفات التنفيذية التي تحتوي شفرة برنامج فيروسي[4]، أو من خلال شبكات إلاتصال[5]، أو عن طريق استخدام قرص مدمج مصاب بالفيروس حيث ينقل الفيروس بمجرد تشغيل القرص المدمج[6]

2. الديدان الألكترونية[7]:

تعرف بأنها(برامج صغيرة قائمة بذاتها وغير معتمدة على غيرها من البرامج، صنعت للقيام بأعمال تدميرية او لسرقة البيانات الخاصة لبعض

(1) للمزيد: د. مصطفى محمد موسى، السيرة الذاتية....، مرجع سابق، ص61.

(2) للمزيد: من هذه البرامج الفيروسية ينظر: خالد ابو الفتوح فضالة، مرجع سابق، ص74. منير محمد الجهني وممدوح محمد الجهني، مرجع سابق، ص54.

(3) د. عمر عبد الفتوح عبد العظيم الحمامي، مرجع سابق، ص265.

(4) د. عادل عزام سقف الحيط، مرجع سابق، ص132.

(5) د. عبد الفتاح بيومي حجازي،الجرائم المستحدثة.....، مرجع سابق، ص507.

(6) د. ايمن عبد الحفيظ عبد الحميد سليمان، أستيراتيجية مكافحة جرائم أستخدام الحاسب الآلي، بدون دار نشر، 2003، ص 293.

(7) ان انتاج اول دودة الكترونية كان عام 1982 لاستخدامها في اعمال مفيدة من قبل شركة (Xerox carp) للقيام بالعمليات التي تحتاج الى التشغيل المتكرر على الحاسبات الرقمية الالكترونية لأكثر من مرة فتقوم الديدان الى مسح الملفات الرقمية المؤقتة التي تنتهي الحاجة منها، و لكن تغير سلوك هذه الديدان وبدأت بتدمير الملفات الموجودة في الجهاز، مما دعى الشركة الى انتاج برنامج مضاد للفيروس، للتخلص من هذه الديدان. ينظر: د. مصطفى محمد موسى، السيرة الذاتية....، مرجع سابق، ص 73 - 74.

المستخدمين اثناء تصفحهم على شبكة الانترنت او ألحاق الضرر بهم او بالمتصلين معهم)، وتتميز الديدان بسرعة الانتشار وصعوبة التخلص منها وقدرتها الفائقة على التلون والتناسخ والمراوغة [1]، و على اعادة توليد نفسها، فهي تلوث كل جهاز متصل بالشبكة حيث تنتقل من ملف إلى آخر ومن جهاز إلى آخر عبر الشبكة[2].

وتتميز الديدان بآلية عمل خاصة بها فهي لا تعتمد على غيرها من البرامج، لأصابة الحاسب الالكتروني إلا أن لكل دودة آلية عمل، فبعضها يقوم بالتناسخ داخل الجهاز الى اعداد هائلة، والبعض الاخر يتخصص بالبريد الالكتروني حيث ترسل الدودة نفسها الى جميع العناوين الموجودة في جهاز المستخدم، أو بالعمل على ارسال رسائل قذرة الى بعض الموجودين في دفتر عناوين الجهاز بأسم مالك البريد الالكتروني مما يسبب له حرج بالغ[3].

وتجدر الاشارة الى ان الديدان الالكترونية قام بصناعتها صانعو برامج الفيروس الا إنها تختلف عن الفيروسات في طريقة انتشارها وكذلك بسرعة انتشارها، فعن طريقة الانتشار تقوم الديدان بنشر نفسها من جهاز الى اخر من خلال شبكة الانترنت، فهي تحاول ان تصيب اكبر عدد من اجهزة الحاسب[4].

اما الفيروسات الالكترونية تحتاج الفيروسات الى تدخل المستخدم لنقلها من حاسب رقمي الى حاسب اخر سواء كان هذا النقل مقصودا أو غير مقصود، فهي تصيب الحاسب عند التخزين عليه من قرص مرن مصاب بالفيروس كما يصاب الحاسوب عن طريق البريد الالكتروني عند استقبال رسالة الكترونية عليه،

---

(1) منير محمد الجهني وممدوح محمد الجهني، مرجع سابق، ص61.

(2) حسن طاهر داوود، الحاسب وأمن المعلومات، معهد الادارة العامة، الرياض، 2000، ص 77 - 78.

(3) منير محمد الجهني وممدوح محمد الجهني، أمن المعلومات الالكتروني، مرجع سابق، ص61. د. عمر ابو الفتوح عبد العظيم الحمامي، مرجع سابق، ص267.

(4) د. ايمن عبد الحفيظ عبد الحميد، مرجع سابق، ص201.

اما عن سرعة كل منها تمتاز الديدان عن الفيروس بأن انتشارها سريع بسرعة انتشار الانترنت [1]، ومن امثلة تلك الديدان التي تنتشر بسرعة انتشار النار في الهشيم ما عرفت باسم (تاناتوس) وكان ظهورها عام 2002، وخلفت وراءها اثار تدميرية هائلة[2]، اما الفيروسات فان سرعة انتشارها تساوي سرعة نقل او تبادل المعلومات[3].

3. حصان طروادة:

يعرف بأنه (برنامج له القدرة على الاختفاء في البرنامج الاصلي للمستخدم وينشط عند تشغيل البرنامج الاصلي، أو هو جزء من الكود يضاف الى البرمجيات ولا يخدم الوظائف العادية التي صنعت من اجلها هذه البرمجيات) [4]، و يؤدي حصان طروادة دورا تخريبيا للنظام، وتكمن خطورة حصان طروادة في عدم علم النظام المعلوماتي بوجوده حتى تحين اللحظة التي يؤدي فيها دوره التخريبي[5]، إذ يتم إدخاله إلى البرامج اثناء تصميمها او تصنيعها من خلال ادخال دوائر سرية بشكل مباشر الى الرقائق التي يتكون منها البرنامج الاصلي[6]، كما ويتم ادخال حصان طروادة من خلال ادخال تعليمات لغة المصدر في وقت لاحق، او عن طريق ادخال التعليمات في لغة الآلة، وجاءت تسمية حصان طروادة من الحصان الخشبي الذي استخدمه الجنود الإغريق للدخول الى حصن طروادة، وهذا التشبيه جاء للتدليل على خطورة البرنامج وقدرته على الخداع والمفاجئة والتضليل[7]، حيث

(1) د. مصطفى محمد موسى، السيرة الذاتية...، مرجع سابق، ص 76 - 78.

(2) منير محمد الجهني وممدوح محمد الجهني، مرجع سابق، ص61.

(3) مصطفى محمد موسى، السيرة الذاتية...، مرجع سابق، ص77.

(4) د. سليم عبد الله الجبوري، الحماية القانونية لمعلومات شبكة الانترنت، ط 1، منشورات الحلبي الحقوقية، بيروت، 2011، ص 328.

(5) حسن طاهر داوود، الحاسب وأمن...، مرجع سابق، ص76.

(6) حسن طاهر داوود، جرائم نظم....، مرجع سابق، ص134.

(7) د. عمر ابو الفتوح عبد العظيم الحمامي، مرجع سابق، ص 242 وما بعدها.

يظهر على انه برنامج صحيح ومفيد يؤدي الاعمال المخصص له ومن ثم يقوم بالاعمال التدميرية[1].

ويستخدم حصان طروادة في عمليات الاختراق، كاختراق البريد الالكتروني، والاستيلاء على الارقام السرية، وعمليات التجسس على الحسابات المالية، وبطاقات الائتمان والتنصت على المحادثات الخاصة والتجسس على خصوصيات الافراد من خلال زرع حصان طروادة في حاسب الضحية[2]، ويستخدم في اختراق المواقع الامنية للدول ومثال على ذلك اختراق الحاسب الالكتروني الخاص بوزارة الدفاع الامريكية البنتاجون[3]،

وهنالك برامج يشبه الى حد ما مع حصان طروادة الا وهو برنامج يطلق عليه القنبلة الموقوتة، ويشتركان في أن كل منهما يعمل على تدمير المعلومات كما أن لهما نفس طريقة البرمجة، أما الفرق بينهما فهو في التصميم، حيت تصمم القنابل الموقوتة ويكون لها أداة موقوتة والتي تتحرك بوقت معين، وتختلف ايضا عن حصان طروادة في كونها تكتشف من قبل برامج المقاومة للبرامج الضارة[4].

أما عن كيفية العدوى بحصان طروادة، فيكون عن طريق البريد الالكتروني حيث يرسل وحيدا أو مع برامج أو ملفات ويقوم المستخدم باستقباله وتشغيله، أو ينتقل عند تحميل برامج من مصادر غير موثوقة، أو عند الاتصال بالشبكات سواء كانت داخلية أو شبكية انترنت[5]، أو عند استخدام برنامج المحادثة الشهير (Ica)

(1) د. احمد محمود مصطفى، جرائم الحاسب الالي في التشريع المصري، ط1، دار النهضة العربية، القاهرة، 2010، ص 234.

(2) د. يوسف حسن يوسف، مرجع سابق، ص 104.

(3) د. عبد الفتاح بيومي حجازي، جرائم الكومبيوتر والانترنت في القانون العربي النموذجي، مرجع سابق، ص94.

(4) د. مصطفى محمد موسى، السيرة الذاتية...، مرجع سابق، ص64.

(5) د. عماد مجدي عبد الملك، مرجع سابق، ص 98.

وهو برنامج محادثة للتجسس من صنع اسرائيل، أو من خلال بعض البرامج المثبتة على الحاسب مثل برنامج الماكرو الموجود في برنامج معالجة النصوص، وينتقل ايضا من خلال برنامج (FTP) او)التلنت) الخاص بنقل الملفات[1]، أو من خلال كتابة كوده على الجهاز نفسه فيتم تحميلة بدقائق قليلة[2].

ولحصان طرواده اشكال متنوعة والتي كانت محل اختلاف بين فقهاء القانون الجنائي، وذلك بخصوص القنابل الالكترونية حيث اعتبارها البعض برنامج متطفل ضار مستقل بذاته، وذهب البعض الى اعتبارها شبيهة ببرنامج حصان طروادة [3] وذهب البعض الآخر إلى القول أن القنابل الالكترونية ماهي إلاّ شكل من اشكال حصان طروادة[4].

فبالنسبة للقنبلة المنطقية هي عبارة عن جزء من رمز والذي يتم ادخاله عمدا الى نظام برمجي ليقوم بأداء مدمر عند اجتماع شروط محددة، ومثاله عمل المبرمج على اخفاء جزء من الشيفرة لتبدء بحذف الملفات تلقائيا إذا ما تم الاستغناء عن خدماته[5] و كذلك قيام أحد العاملين في إدارة المياه والطاقة في ولاية لوس انجلوس الامريكية بوضع قنبلة متطفلة في نظام الحاسب الآلي أدت إلى تخريب هذا النظام عدة مرات[6].

اما القنبلة الزمنية هي عبارة عن كود يتم زرعه في برنامج محدد ويتم برمجته للقيام بهجوم في موعد معين محدد سلفا وهذه المدة قد تطول أو تقصر

---

(1) د. عبد الرحمن جلهم حمزة، جرائم الانترنت من منظور شرعي وقانوني، عدم وجود دار طبع ولا سنة طبع، ص 113.

(2) . يوسف حسن يوسف، مرجع سابق، ص111.

(3) د. مصطفى محمد موسى، السيرة الذاتية...، مرجع سابق، ص64.

(4) د. ايمن عبد الحفيظ عبد الحميد، مرجع سابق، ص303.

(5) د. عادل عزام سقف الحيط، مرجع سابق، ص133.

(6) د. عمر ابو الفتوح عبد العظيم الحمامي، مرجع سابق، ص 253.

حسب رغبة مصمم البرنامج [1]، ومثال على القنبلة الزمنية الجمعة (13) حيث تنشط القنبلة الزمنية في يوم جمعة يصادف (13) لتبدء نشاطها التدميري، وتوجد القنابل الزمنية بكثرة في إسرائيل والولايات المتحدة على الخصوص [2] ومثال على استخدام القنابل الزمنية ماقام به خبير الحاسبات الفرنسي بزرع قنبلة زمنية في حاسب المنشأ الذي يعمل فيه ينفجر بعد مرور ستة أشهر من فصله بدافع الانتقام [3].

خامسا: البريد الالكتروني غير المرغوب فيه[4]:

يعرف بأنه: (عبارة عن رسائل الكترونية دعائية يتم ارسالها عبر البريد الالكتروني (E - Mall))، ويعود ظهور جرائم البريد الالكتروني الى عام 1998، وكان ذلك مرافقا لازدهار التجارة الالكترونية عبر البريد الالكتروني، حيث تقوم الشركات التجارية في محاولة لجذب الزبائن عن طريق الدعاية لمنتجاتها على شبكة الانترنت، وازدادت هذه الدعاية حتى اصبحت كابوسا على مستخدمي الانترنت[5]، حيث ان لكل خدمة حسنة سلبيات ترافقها وسلبيات البريد الالكتروني تتمثل بالرسائل الغير مرغوب فيها، وهي تشبه رسائل الفاكس غير المرغوب فيها كما تشبه المعاكسات الهاتفية، ورسائل البريد الالكتروني هي أما دعائية أو ترويجية للشركات، حيث تقوم هذه الشركات باستغلال البريد الالكتروني للترويج لبضائعها

---

(1) د. ايمن عبد الحفيظ عبد الحميد، مرجع سابق، ص305.

(2) د.عبد الفتاح بيومي حجازي، الجرائم المستحدثة في نطاق تكنولوجيا الاتصالات الحديثة، ط1، المركز القومي للأصدارات القانونية، القاهرة، 2011، ص508.

(3) د. محمود سامي الشوا، مرجع سابق، ص171.

(4) Command of Her Majesty. Cyber Crime Strategy. Presented to Parliament. by the Secretary of State for the Home Department. March 2010.page.10.

(5) د. مصطفى محمد موسى، السيرة الذاتية...، مرجع سابق، ص79.

كالكتب والسيارة وغيرها أو لخدماتها ودعوة الاشخاص للشراء[1]، أو يتمثل في تضخيم البريد الالكتروني من خلال إرسال عدد هائل من الرسائل المكررة والتي تؤدي إلى عدم انتظام سير النظام التقني المعلوماتي، من خلال مواقع النقاش أو مواقع الويب المختلفة[2]، أو إرسال فيروس يستهدف تخريب الحواسيب و الذي يمثل أخطر التهديدات التي تمارس ضد شبكة المعلومات والتي تؤدي الى تلف وتدمير البيانات[3]، أو رسائل تحتوي على صور مخلة بالحياء العام، اذ يتم إرسال صور عارية للأشخاص عن طريق البريد الالكتروني وهو ما قام به مواطن إماراتي بإرسال هذه الصور لكل مشترك يبدء بريده الالكتروني ب(XXZ)[4]، أو تزوير الرسائل الالكترونية حيث يقوم بعض الاشخاص بأرسال رسائل بأسماء اشخاص آخرين عن طريق البريد الالكتروني لا يخرج بعضها عن نطاق التسلية، والبعض الآخر تتسم بالخطورة ويترتب عليها اضرار بالغة[5].

سادسا: برامج التجسس:

تعرف بأنها(اي برنامج يحصل سرا على معلومات عن المستخدم عن طريق الربط بالانترنت، وخاصة بدعاوى دعائية واعلانية، تتخذ شكل برامج مجانية أو برامج مشاركة يمكن تنزيلها من الانترنت)[6].

أو هي (برامج حاسوبية تثبت خفية على أجهزة الكومبيوتر للتجسس على المستخدمين او للسيطرة جزئيا على حواسيب الافراد دون علم المستخدم)، حيث

(1) د. مصطفى محمد موسى، السيرة الذاتية...، مرجع سابق، ص80.
(2) د. خالد ممدوح ابراهيم، التقاضي الالكتروني، مرجع سابق، ص 372 - 374.
(3) د. محمد محمود المكاوي، مرجع سابق، ص126
(4) د. عبد الفتاح بيومي حجازي، الجرائم المستحدثة...، مرجع سابق، ص154.
(5) د. نائلة عادل محمد فريد قورة، مرجع سابق، ص 45.
(6) د. ذيب بن عايض القحطاني، أمن المعلومات، مدينة الملك عبد العزيز للعلوم والتقنية، الرياض، 2015، ص 229.

يقوم بجمع مختلف المعلومات الشخصية مثل تصفح الانترنت، المواقع التي تم زيارتها، كما وتعمل على تغير اعدادات الكومبيوتر لتجعله اكثر عرضة للإصابة بمزيد من الفيروسات[1]، ويكون التجسس من برامج خارجية مبنية على أساس العميل والخادم اذ يعمل برنامج الخادم داخل النظام الحاسوبي للهدف، حتى يتمكن الهكر من الاتصال عن طريقة لتبدء عملية التجسس، هذا النوع من البرامج يعمل على الكومبيوتر الشخصي وقد ظهرت برامج كثيرة للتجسس على أنظمة ويندوز ولينكس[2]، بفتح منفذ في الجهاز المستهدف، ثم استقبال الأوامر من خلال هذا المنفذ، ومن ثم تنفيذ الأوامر التي تأتي من المنفذ[3]، وذلك لإتمام اعمال التجسس العسكري، بالدخول الى حواسيب أجهزة الدولة، او للتجسس على بطاقات الائتمان وأرقام الحسابات، وسرقة البيانات على اختلافها[4].

اما عن طريقة زرع برامج التجسس في حاسب الضحيه، يكون عند زيارة المواقع المجهولة، أو من خلال البريد الالكتروني، أو من خلال برامج المحادثة الشهيرة[5]. ومثال على ذلك برنامج التجسس (icq) الشهير للتجسس، حيث ينتقل الى حاسب الضحيه من خلال الطلب منه ان يضع بياناته على الخادم الخاص بالبرنامج وعند الانتهاء من ملئ البيانات يعطي للمستخدم رقما خاص به مثل رقم التليفون والذي يكون وسيلة للاتصال بالخادم يتيح هذا الرقم لباقي مستخدمي الانترنت ملاحظة وجود المستخدم على الشبكة بمجرد دخوله[6].

(1) عز الدين ابراهيم، نظرة شاملة للحماية من الاختراقات وملفات التجسس Windows، متاح على الموقع www.kutub.com. وقت وتاريخ الزيارة: 1800، 2015/5/16.

(2) للمزيد ينظر: جرائم الكومبيوتر والتجسس الالكتروني الدولي والشخصي للمعلومات. متاح على الموقع الالكتروني: – www.bosla.com. وقت وتاريخ الزيارة: 2050، 2015/5/17.

(3) نهلا عبد القادر المومني، مرجع سابق، ص 218.

(4) ينظر: جرائم الكومبيوتر والتجسس الدولي والشخصي للمعلومات متاح على الموقع الالكتروني. www.boosla.com. وقت وتاريخ الزيارة: 2050، 2015/5/17.

(5) نهلا عبد القادر المومني، مرجع سابق، ص219.

(6) د. ايمن عبد الحفيظ عبد الحميد، مرجع سابق، ص316.

ثانيا: المخاطر الطبيعية:

وتشمل الزلازل والحرائق والفيضانات والتي تدمر النظم المعلوماتية.

فبالنسبة للزلازل تعمل على تدمير المنشأة المعلوماتية بالكامل وغالبا مايصاحب ذلك حريق ينتج عن التماس كهربائي وغيره [1].

أما الفيضانات فهي تسبب عطل كلي أو جزئي للنظم المعلوماتية، ويتوقف تأثير السيول المصاحبة للفيضانات على المنشأة على نوعية ودرجة مقاومة تلك المنشأة للسيول[2].

أما عن الحرائق فلها اثار تدميرية قد تصهر الحديد فكيف الحال يكون بالنسبة للاجهزة المعلوماتية، بالتأكيد لا يمكن الاستفادة منها[3].

(1) منصور بن سعيد القحطاني، مهددات الامن المعلوماتي وسبل مواجهتها، رسالة ماجستير، جامعة نايف العربية للعلوم الامنية، الرياض، 2008، ص 41.

(2) د.خالد ممدوح ابراهيم، التقاضي الالكتروني، مرجع سابق، ص 334. د. أيمن عبد الحفيظ عبد الحميد، مرجع سابق، ص341.

(3) محمد بن فهد الرشيد، البرامج التدريبية ودورها في رفع مستوى الامن المعلوماتي بشركة سابك، رسالة ماجستير، جامعة نايف العربية للعلوم الامنية، 1433، ص32.

الفرع الثاني

المخاطر العامة و المخاطر الخاصة

سوف نتناول أولا المخاطر العامة و ثانيا المخاطر الخاصة التي تتعرض لها البيانات، و على النحو الآتي.

أولا: المخاطر العامة:

وتشمل انقطاع التيار الكهربائي، أو دخول اشخاص غير مخولين إلى النظام المعلوماتي، أو الاعمال الارهابية.

فبالنسبة لأنقطاع التيار الكهربائي، يعتقد البعض أن تعطل الحاسوب يعني ذلك وجود فيروس إلا أن ذلك غير صحيح، فقد يكون بسبب انقطاع التيار الكهربائي بشكل مفاجئ والذي يؤدي إلى انهيار النظام(1)، فانقطاع التيار يسبب أضرارا تفوق بكثير ما يسببه الفيروس الالكتروني(2)، إذ إن لانقطاع التيار الكهربائي آثار مدمرة كآثار الكوارث الطبيعية، ويظهر تأثير انقطاع الكهرباء في مجال المعلومات في جانبين، الأول في فقد المعلومات وذلك قبل حفظها من قبل مستخدم الحاسوب والذي استغرق وقتا طويلا في إعدادها وعدم تمكنه من الحصول عليها بعد فقدانها، والجانب الثاني هو حدوث أخطاء في تشغيل الحاسب وتتمثل هذه الأخطاء بفقد بعض العناقيد أو الفصل بين الملفات المرتبطة(3)، وقد تتعرض أجهزة الحاسب نفسها بما فيها من معلومات للتلف بسبب انقطاع التيار

(1) محمد بن فهد الرشيد، مرجع سابق، ص32.

(2) د. مصطفى محمد موسى، السيرة الذاتية...، مرجع سابق، ص55.

(3) د. ايمن عبد الحفيظ، مرجع سابق، ص 341 - 342.

الكهربائي[1]، وهذا التلف قد يكون جزيئا أو كليا للمعدات المعلوماتية والدعائم التي تختزن المعلومات، أو قد يؤدي الى تعطل المعدات والكيانات المنطقية ولو لفترة قصيرة[2]، وقد هدد خبير كومبيوتر بلجيكي بقطع التيار الكهربائي على بلجيكا من خلال كسر شفرة أجهزة الحاسب الخاصة بمحولات توزيع الكهرباء[3].

أما عن دخول أشخاص من خارج المؤسسة للنظام المعلوماتي، فيكون من خلال دخول أشخاص غير مصرح لهم إلى الحاسب الالي الخاص بالمؤسسات، دخولا مباشرا إلى النظام أو غير مباشر وذلك باعتراض النظام[4]، منتحلين صفة من له حق الدخول إلى النظام المعلوماتي باستغلال بياناته كعنوانه أو رقم الضمان الشخصي..الخ، أو الدخول بانتحال شخصية صاحب الموقع وذلك بتغيره[5]، أو حجبه بعد معرفة كلمة السر الخاصة بالمستخدم وتغيرها مما يؤدي الى عدم استجابه النظام المعلوماتي لصاحبه[6].

أما عن الاعمال الارهابية إذ تقوم بعض المجموعات الإرهابية بحرق المنشآت أو إلقاء القنابل و المتفجرات[7] وذلك لغرض تدمير واتلاف أجهزة الحاسب الآلي[8]، أو القيام باعتداءات من شأنها أن تؤدي الى توقف الحاسب عن العمل بشكل كلي أو جزئي[9].

(1) د. محمد محمود مكاوي، مرجع سابق، ص 265.
(2) د. خالد ممدوح إبراهيم، التقاضي الالكتروني، مرجع سابق، ص 334.
(3) د. حسن المحمدي بوادي، إرهاب الانترنت الخطر القادم، ط1، دار الفكر الجامعي الإسكندرية، 2006، ص 95 - 96.
(4) د. نائلة عادل محمد فريد، مرجع سابق، ص 338.
(5) د. عفيفي كامل عفيفي، مرجع سابق، ص 465 - 466.
(6) جلال محمد الزعبي و اسامة احمد المناعسة، مرجع سابق، ص 251.
(7) د. ايمن عبد الحفيظ، مرجع سابق، ص 330.
(8) د. محمد محمود مكاوي، مرجع سابق، ص 265.
(9) منصور بن سعيد القحطاني، مرجع سابق، ص 41.

ثانيا: المخاطر الخاصة:

وتتمثل هذه المخاطر باخطاء المستخدمين، والتي تنقسم إلى الخطأ في تشغيل النظام المعلوماتي، مما يلحق الضرر بالمعلومات الناتجة عن التشغيل، أو عدم خبرة المستخدمين والذي يؤدي إلى فتح أبواب لدخول المتسللين إلى أنظمة الكومبيوتر، أو مسح الملفات أو عدم حفظها والذي يؤدي إلى عدم إمكانية استعادتها مرة أخرى، أو قيام الموظفين بالعبث في تشغيل البيانات من خلال القيام بالنسخ الغير قانوني للبيانات وتحريفها وسرقتها، كاعطاء أوامر للبرنامج غير مصرح به، كعدم تسجيل أي قيد بالسجلات المالية الخاصة بعميل معين للاستفادة من المبلغ لصالحه[1]، أو قيام الموظف بالدخول إلى النظام المعلوماتي بكلمة المرور بعد سرقته لها لتحقيق مصالح معينة[2]، أو استنزاف وقت العمل بقيام الموظف بالتصفح في شبكة الانترنت أثناء الدوام الرسمي.

نخلص مماتقدم أن هنالك برامج ضارة لا حصر لها، تختلف في طرق أصابتها وتأثيرها وكيفية التخلص منها، بعضها يقف أثرها عند الازعاج والبعض الآخر لها آثار مدمرة للحاسبات أو الشبكات أو الانظمة المعلوماتية..الخ، كما تتعرض المباني بما تحوية من نظم معلوماتية، إلى المخاطر الطبيعية والعامة والتي لها أضرار تفوق أضرار البرامج الفيروسية وغيرها، مما يجعل من الضروري أن تبنى المؤسسات في أماكن تقل بها الزلازل أو الفيضانات..الخ، وأن تضع هذة المؤسسات نظم أطفاء وفرق للحماية من أجل حماية هذة النظم المعلوماتية وتقليل الخسائر.

(1) د. خالد بن سليمان الغثبر و د. محمد بن عبد الله القحطاني، أمن المعلومات بلغة ميسرة، ط1، مكتبة الملك فهد الوطنية، الرياض، 2009، ص 26 وما بعدها. حسن طاهر داود، الحاسب وامن المعلومات، مرجع سابق، ص 23 وما بعدها. محمد بن فهد الرشيد، مرجع سابق، ص 40.

(2) منصور بن سعيد القحطاني، مرجع سابق، ص 41.

المطلب الثاني

الأمن المعلوماتي

ويقصد بالأمن المعلوماتي من ناحية مادية وغير مادية:

(مجموعة من الإجـراءات الإدارية والفنية التي صممت لضمان حماية الأجهزة وملحقاتها والبرامج والبيانات من السرقة أو التوقف أو التلف المتعمد أو غير المتعمد أو التخريب أو التبديل أو مجرد الاطلاع دون تصريح بالاستخدام، وحماية شبكة المعلومات الداخلية والاتصالات الخارجية من الاختراق أو التعطيل المتعمد أو غير المتعمد)(1)، أما من ناحية تقنية فيقصد به (الوسائل والادوات والاجـراءات التي من الضروري توفيرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية)(2).

وتنبثق أهمية أمن المعلومات من كونها تمثل قيمة مادية ومعنوية للأفراد والمنظمات والشركات والدول(3)، وأنها هدف للاختراق من قبل نفس الأشخاص، فكان لا بد من تعريف مستخدمي نظم المعلومات وجميع الموظفين الذين يعملون في نظم المعلومات بواجباتهم المطلوبه، لحماية نظم الحواسيب والشبكات وبالاجراءات التي يجب أتباعها لتفادي التهديدات والمخاطر وكيفية التعامل معها، لما تمثله المعلومة من سلاح للانتصار او الانهزام في حرب المعلومات، والتي تكون هي الفيصل في الكسب أو الخسارة للشركات والتي تكلف الفرد ثروته أو حياته في

(1) منصور بن سعيد القحطاني، مرجع سابق، ص 19.

(2) حرية شعبان محمد الشريف، مخاطر نظم المعلومات والمحاسبية الالكترونية، رسالة ماجستير، الجامعة الاسلامية غزة، 2006، ص 64.

(3) محمد بن فهد الرشيد، مرجع سابق، ص27.

بعض الأحيان. ولأهمية المعلومات اتجهت الدول والشركات والمبرمجون الى صناعة الوسائل الكفيلة بتوفير الحماية للمعلومات[1].

وعليه سنبين في هذا المطلب النظم التقليدية في تأمين البيانات والنظم التقنية الحديثة في تأمينها.

(1) حرية شعبان محمد الشريف، مصدر سابق، ص68.

الفرع الأول

النظم التقليدية في تأمين البيانات

من النظم التقليدية في التأمين هي التشفير والتوقيع الرقمي وكلمة السر.

فبالنسبة للتشفير: (هو عملية تحويل البيانات المعالجة ألكترونيا إلى رموز لعدم تمكن الغير من انتهاك سريتها[1]، إذ إن برمجيات التشفير تتضمن نوعين من الإجراءات، الأولى تحويل البيانات أو المعلومات إلى رموز، والثانية تحويل الرموز إلى بيانات أو معلومات وذلك بفك الشفرة)[2].

ويعرف أيضا (بأنه علم الكتابة السرية المتضمن العمل على أخفاء المعلومات الموثوقة، بطريقة معينة بحيث يكون معناها غير مفهوم للشخص غير المخول)[3]، ويعمل التشفير على منع الغير من الدخول أو التعامل مع المواقع الالكترونية، أو الحصول على الخدمات إلا بتصريح من المالك[4].

وإذا كانت الغاية او العلة من التشفير هو حماية البيانات المتداولة على شبكة الانترنت لحماية العمليات التجارية والصناعية والأمنية... الخ، والحفاظ على سرية هذه البيانات من اطلاع الغير عليها[5]. نطرح سؤالا هل لهذه التقنية من سلبيات،

(1) Understanding EncryptionAvailable.on thewebsite. https: www. securing thehuman. sans. org. Date 30 - 12 - 2015

(2) د. عبد الفتاح بيومي حجازي، نحو صياغة نظرية عامة في علم الجريمة والمجرم المعلوماتي، ط 1، منشأة المعارف، الاسكندرية، 2009، ص73 - 76.

(3) عبد الصبور عبد القوي علي مصري، التنظيم القانوني للتجارة الالكترونية، مكتبة القانون والاقتصاد، الرياض، 2012، ص 341.

(4) د. محمد محمود المكاوي، مرجع سابق، ص271.

(5) د. هدى حامد قشقوش، الحماية الجنائية للتجارة الالكترونية عبر الانترنت، دار النهضة العربية، القاهرة، 2000، ص 41.

والجـواب يكون نعم، حيث تستخدم عملية التشفير من قبل عصابات الجريمة المنظمة وذلك بتشفير الاتصالات فيما بين كبار مسؤولي الجرم المنظم وكذلك مع المنفذين لعمليات التجسس والتخابر الأمني والارهابي على شبكة الانترنت[1]، إذ تعمل منظمات المخدرات والمؤثرات العقلية باستخدام عملية التشفير، في انجاز صفقاتها غير المشروعة عبر الانترنت، وقيام المؤسسات الاقتصادية بتشفير بياناتها بهدف التهرب الضريبي[2].

يضاف إلى ماتقدم أن وجود شفرات المرور أو شفرات ترميز البيانات يصعب من مهمة المحقق في اكتشاف الجريمة[3]، ومثال على ذلك ما حدث في قضية السيد (فورسن) وهو شاب يسكن الولايات المتحدة الامريكية، حيث نشر على أحد مواقع الانترنت رسالة عنصرية ضد أحد اليهود، والتي تحمل اسمه (روبورت فورسن)، و لم تستطع المحكمة من إقامة الدليل عليه، لاستخدام التشفير في الحادثة، وقالت المحكمة أن مجرد وجود اسم الشخص لا تعني أنها صادرة عنه [4].

وللتشفير أنـواع متعددة نذكر هنا أبـرز أنواعه والتي وجـدت أساسها في عمليات التشفير المستخدمة قديما منذ الحرب العالمية الأولى والثانية، حيث كانت خطط الحرب وطرق الهجوم ترسل باليد ولكن مشفرة بإحدى طرق التشفير[5] وكما يلي.

---

(1) عادل عبد الجواد محمد الكردوسي، التعاون الامني العربي ومكافحة الاجرام المنظم عبر الوطنية، مكتب الاداب، القاهرة، 2005، ص123.

(2) د. محمد محمود مكاوي، مرجع سابق، ص273 - 274.

(3) د. عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية، ط 1، دار النهضة العربية، القاهرة، 2009، ص268.

(4) د. سليمان احمد فضل، مرجع سابق. ص376.

(5) وجدي عصام عبد الرحمن، التشفير بالطرق الكلاسيكية، 2007، ص2. بحث متاح على الموقع الالكتروني www.pdffactory.com. وقت وتاريخ الزيارة: 2000، 2015/7/6.

التشفير المتماثل (أو المتناظر) والذي هو عبارة عن استخدام مفتاح سري واحد معروف لدى الطرفين (المرسل والمستقبل للبيانات)، ويجب عدم اطلاع الشخص الآخر عليه[1]، أو هو استخدم مفتاح مع خوارزمية لتشفير المعلومات واستخدام نفس المفتاح ونفس الخوارزمية لفك التشفير ومن هنا جاءت التسمية[2]، حيث تتضمن كلمة المرور التي سيتم استخدامها لفك التشفير على حروف كبيرة وصغيرة ورموز وتقوم بعد ذلك برمجيات التشفير بتحويل كلمة المرور إلى عدد ثنائي ويشكل العدد الثنائي الناتج مفتاح تشفير الرسالة وتقوم البرمجيات مرة أخرى بإعادة النص إلى أصله بترجمة المفتاح الثنائي[3].

أما التشفير غير المتماثل (او غير المتناظر)، والذي هو النوع الثاني من التشفير والذي يتم باستخدام مفتاحين أحدهما عام معروف لدى المستخدمين والآخر خاص ويتم فيه فك تشفير البيانات[4]، إذ يحقق هذا النوع من التشفير أمانا أكثر من التشفير المتماثل، إذ إن في التشفير المتناظر يستطيع المخترق الوصول إلى المفتاح عن طريق الدليل العام أو عن طريق شخص آخر[5] أما في التشفير غير المتماثل لا يستطيع فك الشفرة بالحصول على المفتاح العام إذ لا بد من الحصول على المفتاح الخاص[6].

(1) د. نعيم مغبغب، حماية برامج الكومبيوتر الأساليب والثغرات، ط2، منشورات الحلبي الحقوقية، بيروت، 2009، ص 250.

(2) وجدي عصام عبد الرحمن، مرجع سابق، ص 87.

(3) محمد الكشبور، المعاملات والإثبات في مجال الاتصالات الحديثة، سلسلة الدراسات القانونية المعاصرة، مطبعة النجاح – الدار البيضاء، العدد12، 2007، ص38.

(4) كوثر مازوني، الشبكة الرقمية وعلاقاتها بالملكية الفكرية، دار الجامعة الجديدة، الاسكندرية، 2008، ص284. اريك ليوبولد – سيرج لوت، ترجمة فتحي علي، أمن المعلومات، مدينة عبد العزيز للعلوم والتقنية، الرياض، 2014، ص 70.

(5) المعرفة القانونية، موقع ويكيبيديا، الموسوعة الحرة،، وقت وتاريخ الزيارة:2300، 2015/6/5.

(6) د. عبد الفتاح بيومي حجازي، مكافحة جرائم الكومبيوتر والانترنت...، مرجع سابق، ص 49.

ومن الجدير بالاشارة إذا كان استخدام البرمجة في التشفير هو الشائع فإن ذلك لا يمنع من استخدام آلات وقطع صلبة مصممة خصيصا للتشفير(1). ويعد التشفير المتماثل والغير متماثل من أهم وسائل تأمين البريد الإلكتروني على الاطلاق(2).

ومن الجدير بالذكر هنالك قواعد تحكم عملية التشفير، ومن هذة القواعد عدم وجود ما يمنع من تشفير البيانات(3).

وقد أخذ بهذه القاعدة قانون التجارة الألكتروني الأتحادي الاماراتي رقم (1) لسنة 2006 حيث نصت المادة (17) على أن " 2 - يعتبر الاعتماد على التوقيع الالكتروني المحمي معقولا مالم يثبت العكس "، حيث يعد التشفير الالكتروني من وسائل الحماية، وأخذ بهذه القاعدة أيضا قانون التجارة الالكترونية الأمريكي الصادر عام 2000، وهو ما تبناه المشرع الفرنسي كذلك حيث سمح للمشروعات الصغيرة بتشفير بياناتها بمقتضى القانون الصدر عام 1990 بعد أن كان التشفير قاصرا على المجالات العسكرية والدبلوماسية والحكومية(4). والقاعدة الثانية هي أحترام سرية البيانات أذ من حق أصحاب البيانات المشفرة الحفاظ على خصوصيتهم وعدم فضها الا بموجب تصريح كتابي من صاحب الشأن(5)، حيث نظمت بعض الدول عملية التشفير وجرمت كل فعل يمثل اعتداء على البيانات المشفرة، ومن بين هذة الدول الامارات العربية المتحدة وامريكا حيث عاقبت على فض البيانات المشفرة وأكدت فرنسا ان الاعتداء على البيانات المشفرة دليل على توافر الركن المعنوي لدى الجاني(6)، وعاقبت المادة (22) من القانون

(1) د. محمد محمود مكاوي، مرجع سابق، ص472 - 273

(2) د. نعيم مغبغب، حماية برامج الكومبيوتر...، مرجع سابق، ص 250.

(3) د. عبد الفتاح بيومي حجازي، الجرائم المستحدثة....، مرجع سابق، ص71 - 72.

(4) كوثر مازوني، مرجع سابق، ص284.

(5) د. هدى حامد قشقوش، مرجع سابق، ص60.

(6) د. عبد الفتاح بيومي حجازي،الجرائم المستحدثة...، مرجع سابق، ص72.

الاتحادي لدولة الامارات على الدخول بغير وجه حق الى النظام المعلوماتي بقصد الحصول على البيانات أو المعلومات الحكومية السرية سواء كانت سرية بطبيعتها او بمقتضى التعليمات[1]. ومن القواعد أيضا الحصول على اذن بالتشفير لكي تكون عملية تشفير البيانات مشروعة لابد من حصول اذنٍ بذلك، وقد أوكل القانون الفرنسي هذه المسألة بوزارة الاتصالات الفرنسية أو رئيس الوزراء الفرنسي في بعض الأحيان، وقد خصت إمارة دبي أمر الاذن بالترخيص والاشراف على عمليات توريد أجهزة التشفير وتشغيلها من قبل مراقب خدمات التصديق[2]، ولخطورة التشفير واسهامه في تسهيل الأنشطة الأجرامية قامت بعض الدول بانشاء مكاتب متخصصة ملتزمة بالسرية، يودع لديها مفاتيح التشفير[3]، حيث كان ضروريا حصر عملية التشفير بسلطة مختصة، و أوكلت بعض الدول مسألة منح الإذن بعدة جهات أمنية حفاظا على أمنها القومي[4]. وأرى أن هنالك تقاطع بين القاعدة الاولى والمتضمنه عدم وجود مايمنع من التشفير، والقاعدة الثالثة التي تأكد على ضرورة الحصول على أذن بالتشفير، ومن وجهة نظري أن القاعدة الثالثة هي الافضل للتقيليل من مخاطر التشفير وذلك بأخضاع عملية التشفير لرقابة الدولة.

أما التوقيع الالكتروني فقد عرفه قانون التوقيع الالكتروني والمعاملات الالكترونية العراقي رقم (78) لعام 2012 حيث نصت (الفقرة رابعا من المادة 1) على أن " علامة شخصية تتخذ شكل حروف أو أرقام أو رموز أو إشارات أو أصوات أو غيرها وله طابع منفرد يدل على نسبته الى الموقع ويكون معتمد من جهة التصديق ".

(1) علي عدنان الفيل، الاجرام الالكتروني، ط1 ،منشورات الحلبي الحقوقية، بيروت، 2011،ص 183.

(2) د. عبد الفتاح البيومي حجازي، الجرائم المستحدثة....، مصدر سابق، ص 72 هامش (3).

(3) د. سليمان احمد فضل، مرجع سابق، ص 378.

(4) د. محمد امين الرومي، التنظيم القانوني للاتصالات في مصر والدول العربية، ط1، دار الكتب القانونية، القاهرة، 2008، ص207 وما بعدها.

وعرفت المادة (1) من القانون الاتحادي الاماراتي الخاص بالمعاملات والتجارة الالكترونية رقم (1) لسنة 2006 التوقيع الالكتروني بأنه" التوقيع المكون من حروف وأرقام أو رموز أو صوت أو نظام معالجة ذي شكل الكتروني وملحق أو مرتبط منطقيا برسالة الكترونية وممهور بنية توثيق أو اعتماد تلك الرسالة".

كما عرفه قانون التوقيع الالكتروني الامريكي رقم (761 د) لسنة 2000 بأنه" شهادة رقمية تصدر عن إحدى الهيئات المستقلة، وتميز المستخدم عن غيره عند إرساله رسالة أو عقد تجاري أو تعهد أو إقرار" [1].

ويعرف أيضا (عبارة عن حروف أو أرقام أو رموز أو إشارات لها طابع منفرد، تسمح بتحديد الشخص صاحب التوقيع وتميزه عن غيره، وهو الوسيلة الضرورية للمعاملات الالكترونية في إبرامها و تنفيذها، والمحافظة على سريتها وسرية الرسائل)[2].

ويستخدم التشفير لتأمين ما يعرف بالتوقيع الرقمي أو الكودي[3]، فالتوقيع رسالة فعالة في حماية اعتبارات الأمن والخصوصية على شبكة الانترنت، فباتت المعلومات السرية الخاصة بالحكومة الالكترونية، ومعلومات التجارة الالكترونية على درجة من الأمان[4]، فالتوقيع الرقمي يحقق حماية وأمنا أكثر مما يحققه

(1) أشار اليه: د. عبد الفتاح بيومي حجازي، مكافحة جرائم الكومبيوتر والانترنت في القانون العربي النموذجي، ط1، دار الفكر الجامعي، الاسكندرية، 2006، ص 73 - 74.

(2) د. محمد حسين منصور، المسؤولية الالكترونية، ط1، منشأة المعارف، الاسكندرية، 2006، ص 151. د.علوطي لمين، تحديات الامن الالكتروني في المؤسسة، أبحاث أقتصادية وأدارية، جامعة محمد خيضر - الجزائر، العدد 7، 2009، ص 173.

(3) د. عبد الفتاح بيومي حجازي،الحكومة الالكترونية بين الواقع والطموح، ط 1، دار الفكر الجامعي، الاسكندرية، 2009، ص524.

(4) د. عبد الفتاح بيومي حجازي، مكافحة جرائم الكومبيوتر و الانترنت في القانون العربي النموذجي، مرجع سابق، ص73 - 74.

التوقيع العادي، وذلك لأن الأخير عبارة عن رسم يقوم به شخص فهو فن وليس علم ومن هنا يسهل تزويره، أما التوقيع الرقمي فإنه علم تستخدم فيه تقنيات التشفير وليس فن، ومن ثم يصعب تزويره[1].

وللتوقيع الالكتروني صور منها:

- **التوقيع بالقلم الالكتروني** حيث يتم التوقيع على شاشة الكومبيوتر، باستخدام قلم الكتروني حسابي و باستخدام برنامج معين، حيث يقوم هذا البرنامج بوظيفتين الأولى خدمة التقاط توقيع العميل، والثانية خدمة التحقق من صحة التوقيع[2].
- **أما الصورة الثانية هي التوقيع الرقمي أو الكود**، هو توقيع يتكون من عدة أرقام يتم تركيبها بطريقة معينة في شكل كود يقوم بوظيفة التوقيع[3]، ويعتبر التوقيع الرقمي المقابل للتوقيع المعتاد، وفائدته تتمثل في التحقق من شخصية المرسل[4]، ويتم انشاء هذا التوقيع عن طريق تشفير القيمة الاختبارية المنتجة من الرسالة باستخدام المفتاح السري للمرسل ويتكون بذلك التوقيع الرقمي[5]، وهو أسلوب يستخدم في المعاملات البنكية كبطاقات الائتمان[6].

(1) محمد الكشبور، مرجع سابق، ص31. حسن طاهر داود، جرائم نظم المعلومات، ص107.
(2) منير محمد الجهني و ممدوح محمد الجهني، الشركات الالكترونية، دار الفكر الجامعي الاسكندرية، 2005، ص 140. د. هدى حامد قشقوش، مرجع سابق، ص77 - 78.
(3) كوثر مازوني، مرجع سابق، هامش ص 290.
(4) حسن طاهر داود، جرائم نظم المعلومات، مرجع سابق، ص107.
(5) د. نعيم مغبغب، حماية برامج الكومبيوتر...، مرجع سابق، ص251.
(6) د. هدى حامد قشقوش، مرجع سابق، ص 75.

ومن الجدير بالذكر أطلق مشروع قانون مكافحة الجرائم المعلوماتي العراقي لعام 2012 [1] على كلمة السر عبارة " بيانات المرور".

و عرفها (بالفقرة السادسة من المادة 1) حيث نصت على أن " الرموز أو الارقام الخاصة بالدخول للشبكات والاجهزة والحاسبات أو أية بيانات تعريفية مشابهة ترسل من أو إلى نقطة اتصالية بما في ذلك تاريخ وحجم ووقت الاتصال وأية معلومات تحدد الموقع الذي يتم منه أو إليه نقل البيانات بأي نمط من أنماط الاتصالات بما فيها الاتصالات الخلوية ".

وعرفها مشروع قانون مكافحة جرائم الكومبيوتر والانترنت العربي النموذجي بأنها" كلمة يحتفظ بها مستخدم الحاسب سرا ويطلبها الحاسب منه قبل التعامل للتأكد من هويته" [2].

وعرفت أيضا بأنها (رقم أو كلمة سرية والتي تمنع أي تعامل مع النظام المعلوماتي إلا بذكرها)[3]. وتعد كلمة السر أحدى الوسائل الفنية لحماية شبكة المعلومات في النظام المعلوماتي، وكذلك في حماية الحاسب الشخصي، ويعد هذا الأسلوب من أسهل وأرخص أساليب حماية البيانات والمعلومات[4].

إن كلمة السر لا تعد كافية لحماية البيانات والمعلومات إذ يوجد هنالك جهاز يقوم بعدد لا متناهٍ من المحاولات حتى يصل إلى الكلمة الصحيحة[5]، أو مراقبة

---

(1) جاء مشروع قانون الجرائم المعلوماتية العراقي لعام 2012 خاليا من عقوبات، في حين تضمن مشروع قانون الجرائم المعلوماتية لعام 2010 عقوبات.

(2) أشار اليه: د. عبد الفتاح بيومي حجازي، مكافحة جرائم الكومبيوتر والانترنت..، مرجع سابق، ص58.

(3) نهلا عبدالقادر المومني، مرجع سابق، ص220.

(4) للمزيد: د. عبد الفتاح بيومي حجازي، نحو صياغة نظرية عامة في علم الجريمة والمجرم المعلوماتي، منشأة المعارف، الاسكندرية، 2008، ص57.

(5) د. عبد الفتاح بيومي حجازي، مكافحة جرائم الكومبيوتر والانترنت في القانون العربي..، مرجع سابق، ص 59.

ضغط الأصابع من قبل المقتحم، أو توقع كلمة المرور[1]، إلا أن هنالك بعضَ الأمور تحول دون الوصول ألى كلمة السر، منها تحديد عدد المحاولات الفاشلة، والتي بعدها يتم فصل الطرفية وايقافها عن العمل تماما[2]، أو عدم كتابة كلمة سر تشير إلى اسم مستخدم الجهاز أو ميلاده أو أي شيء مشهور به، وعدم الرجوع الى كلمة سر سابقة استخدمها من قبل وجرى التحديث عليها من قبل صاحب الجهاز[3]، كما يجب عدم عرض حروف كلمة السر أثناء كتابتها، حتى لا تعرف من قبل المتطفلين، وكتابة كلمة سر طويلة نسبيا تتكون من أرقام وحروف وعلامات ترقيم وعدم الإفصاح عنها لأي شخص[4].

وأخيرا فعلى الرغم من سلبيات برنامج الوصول إلى كلمة السر، إلا أنه لا يخلو من فائدة حيث يساعدنا على معرفة كلمة السر المنسية، أو لتخفيف الأضرار في حال تعمد اغلاق الملفات بكلمة سر[5].

(1) د. عبد الفتاح بيومي حجازي، نحو صياغة....، مرجع سابق، ص381.

(2) حسن طاهر داود، الحاسب وامن المعلومات، مرجع سابق، ص310 - 311.

(3) د. علوطي لمين، مرجع سابق، ص176.

(4) د. ايمن عبد الحفيظ عبد الحميد سلمان، مرجع سابق، ص 380.

(5) د. مصطفى محمد موسى، الجهاز الالكتروني لمكافحة الجريمة، دار الكتب القانونية، القاهرة، 2006، ص 169 - 170. د. عبد الفتاح بيومي حجازي، مكافحة جرائم الكومبيوتر والانترنت في القانون العربي....، مرجع سابق، ص59.

الفرع الثاني

النظم التقنية الحديثة في تأمين البيانات

بالرغم مما تحققه الوسائل التقليدية في تأمين البيانات إلا أنها تبقى قاصرة عن مواجهة كافة الاعتداءات التي تتعرض لها أجهزة الحاسب الالي وما تحويه من معلومات و برامج، مما دعى إلى تطوير وسائل تقنية وإلى إيجاد طرق جيدة في هذا الصدد، ومنها برامج الجدار الناري، و الشبكة الافتراضية، وأجهزة الخصائص البيولوجية.

فبالنسبة لجدران الحماية (الجدار الناري) هو عبارة عن برامج أو جهاز يوفر سياجا امنيا ما بين الحاسب الآلي وشبكة الانترنت، أو شبكة حاسبات أو بين شبكة حاسبات وأخرى، حتى يتم اخضاع جميع عمليات الدخول والخروج من وإلى الشبكة لسيطرة الجدار الناري[(1)]، لمنع دخول المتطفلين والبرامج الضارة إلى الحاسب الالكتروني[(2)]، فهو جواز مرور للبيانات المتبادلة بين الشبكة الداخلية المحمية والشبكات الخارجية التي يخشى منها، وتتناول سياسة المنع عدم السماح بالدخول من الخارج والسماح بالمرور إلى الخارج، أو السماح بدخول أشخاص معينين أو نشاطات معينة أو الدخول من مكان معين[(3)]، وظهر أول جدار حماية للشبكات في عام 1980 وكانت بسيط وفعال من خلال تعريفها على عدد محدد من الأشخاص المسموح لهم بالمرور، كما يعمل على تقسيم الشبكات إلى أجزاء وعزل

(1) د. عبد الفتاح بيومي حجازي، الحكومة الالكترونية....، مرجع سابق، ص220.

(2) حسن طاهر داود، جرائم نظم المعلومات، مرجع سابق، ص109.

(3) د. نعيم مغبغب، حماية برامج الكومبيوتر...، مرجع سابق، ص 213.

الأجزاء المصابة منها، لوقاية الأجزاء السليمة من أن تنتقل إليها الإصابة [1]، ويؤدي جدران الحماية عمله من خلال حاسب خارج الحاسب الرئيسي للمؤسسة[2]. وعمل صانعو برامج الحماية إلى تطويره وإضافة بعض البرمجيات، لإنجاز مهامه على أفضل صورة مثل برمجيات مراقبة المحتوى، حيث يعمل جدران الحماية على مراقبة المحتوى الوارد الى الشبكة، والبحث عن الفيروس..الخ، وكذلك التحقق من هوية المستخدم باستخدام أساليب التشفير مثل الشهادة الرقمية، والتي يمكن من خلالها تفادي هجمات إعادة الاستخدام وبرمجيات حساب الشفرة الرقمية الخاصة[3]، أو إضافة الجدار الناري الخاص، والذي هو جيل جديد من الجداران النارية، يعمل على معالجة الأجزاء المصابة في نظام التشغيل دون الحاجة إلى تدخل المستخدم[4]، أو استخدام الشبكات الافتراضية الخاصة، والتي يتم انشاؤها على ظهر الشبكة الأم، تخدم عدد من المستخدمين لا يستطيع أحد أو طرف استخدامها غيرهم[5].

ولجدران الحماية أنواع منها، الموجه الحاجب والذي يعتبر من أبسط أنواع جدران الحماية، والأكثر فعالية في بعض المواقف، حيث يعمل ما بين الحاسبات المضيفة والشبكات الكبيرة، ولا يرى هذا النوع من جدران الحماية سوى العناوين ونوع البروتكول المستخدم فيه و لا يرى المحتوى، لذا عملية الرقابة على الأنشطة تكون صعبة[6].

(1) منير محمد الجهني وممدوح محمد الجهني، أمن المعلومات الالكتروني، دار الفكر الجامعي، الاسكندرية، 2005، ص65.

(2) د. عبد الفتاح بيومي حجازي، نحو صياغة....، مرجع سابق، ص329.

(3) د. محمد محمود المكاوي، مرجع سابق، ص 286.

(4) منير محمد الجهني وممدوح محمد الجهني، أمن المعلومات الالكتروني، مرجع سابق،ص 68.

(5) د. ايمن عبد الحفيظ عبد الحميد سليمان، مرجع سابق، ص398.

(6) حسن طاهر داود، جرائم نظم المعلومات، مرجع سابق، ص162 - 175.

أما بالنسبة لبرنامج الوسيط فهو عبارة عن كومبيوتر يقوم بتطبيق بروتكول خاص بموجه، يسمح بمرور بيانات معينة مسموح لها بالمرور ويضعها في تصرف المستفيد، فهو يرى النص الكامل للرسائل ويعمل على توظيفها إذ يعمل بالنيابة عن المستفيد، ويرفض ما هو غير متوافق مع نظام الجدار حيث يوفر درجة كبيرة من الأمان للمعلومات، ويستخدم هذا الجدار من قبل المؤسسات والمستشفيات والمدارس... الخ[1] و من الشركات و الدوائر الحكومية[2].

أما عن برنامج الحارس، هو برنامج وسيط متطور، حيث تمت إعادة كتابة جزء من الكود الخاص بالبرنامج الوسيط، ويعتبر هذا البرنامج الوحيد الذي له القدرة على مخاطبة الانترنت، ويحوي أيضا بوابة للفلترة ومشبك داخلي للبريد.[3] ويعتبر أكثر تعقيدا حيث هو الذي يقرر بنفسه السماح بمرور البيانات أو منعها[4] كما يحدد الخدمات التي يقوم بها نيابة عن المستفيد اعتمادا على المعلومات المتاحة، مثل التعرف على شخصية المستفيد الخارجي أو تحديد التعاملات السابقة[5].

ورغم مزايا جدران الحماية المتمثلة بتوفير الحماية اللازمة للشبكات والبيانات والحد من تعرضها للاختراق، كونه المسؤول عن عملية الدخول والخروج عبر الشبكات للبيانات[6]، فأن له عيوباً أهمها أن استخدامه يؤدي الى بطء التعامل مع شبكة الانترنت، ورفض بعض المعلومات الآمنة التي يحتاج اليها المستخدمون داخل المؤسسات أو الشركات[7]، كما لا تقدم الحماية الكافية لمحتوى البيانات التي

(1) د. نعيم مغبغب، حماية برامج الكومبيوتر...، مرجع سابق، ص 215.

(2) للمزيد: حسن طاهر داود، جرائم نظم المعلومات، مرجع سابق، ص169.

(3) منير محمد الجهني وممدوح محمد الجهني، أمن المعلومات الالكتروني، مرجع سابق، ص66.

(4) د. نعيم مغبغب، حماية برامج الكومبيوتر...، مرجع سابق، ص216.

(5) حسن طاهر داود، جرائم نظم المعلومات، مرجع سابق، ص173.

(6) المعرفة القانونية، موقع ويكيبيديا، الموسوعة الحرة،، وقت وتاريخ الزيارة: 2300، 2015/6/5.

(7) د. ايمن عبد الحفيظ عبد الحميد سليمان، مرجع سابق، ص 395.

يتم تمريرها إلى الداخل والتي تتضمن معلومات غير صحيحة أو برامج ضارة لوجوده خارج حدود الشبكة، كما لا يمنع المهاجم من الداخل والذي يريد سرقة بعض البيانات[1].

أما الشبكة الافتراضية فهي شبكة خاصة بشركة أو منشأة او هيأة يتم انشاؤها فوق شبكة عامة، مستفيدا من الشبكة العامة وتعمل على أسس فنية مختلفة، حيث يتم استثمار الشبكة المتاحة بإنشاء قنوات اتصال خاصة، كشبكة منفصلة ببعض من المستخدمين وتكون مغلقة عليهم لا يستطيع أي أحد الدخول إليها، وسميت بالافتراضية لأن ليس لها وجود مادي وأنها لا تستمر لوقت طويل وإن كان بعضها مستمرا[2].

ويوجد هنالك أربعة مستويات لتأمين الشبكة، المستوى الأول نظام الشبكة الافتراضية الخاصة والتي تستخدم التشفير في تأمين البيانات والمعلومات المنقولة عبر شبكة الانترنت[3]، وهذا النوع من التأمين للبيانات أصبحت برمجيات تضاف إلى جدران الحماية، لزيادة فاعليتها في تأمين البيانات المتبادلة عبر الشبكة[4]، وعن المستوى الثاني هو نظام نت سكيب للتأمين، حيث يتم تشفير جميع الاتصالات بين إحدى برامج التصفح وإحدى المعلومات على خادم الشبكة[5]، أما عن المستوى الثالث نظام بروتوكول نظام الأفق، والذي يقوم بتشفير البيانات المدخلة بالمتصفح اثناء نقلها بين جهاز المرسل والمستقبل[6]، ويختلف هذا النظام عن نظام نت سكيب

---

(1) للمزيد: حسن طاهر داود، الحاسب وامن المعلومات، مرجع سابق، ص361.

(2) د. ايمن عبد الحفيظ عبد الحميد سلمان، مرجع سابق، ص398.

(3) منير محمد الجهني وممدوح محمد الجهني، مرجع سابق، ص68.

(4) د. محمد محمود مكاوي، مرجع سابق، ص287.

(5) محمد امين الرومي، مرجع سابق، ص 210.

(6) جريدة الرياض، امن الشبكات اللاسلكية وسبل حمايتها، متاحة على الموقع www.alriyadh.com. وقت وتاريخ الزيارة: 2100، 2015/7/15.

في أن نظام نت سكيب يقوم بحماية البيانات ذاتها بينما نظام البرتوكول يقوم بحماية قنوات الاتصال، وعن المستوى الرابع نظام تأمين المعاملات الالكترونية، يعمل هذا النظام على تأمين العمليات المالية والتي تتم عبر شبكة الانترنت ويستخدم هذا النظام عدة مستويات من التشفير[1].

وللشبكة الافتراضية الخاصة فوائد فهي تأمين الاتصال بين مجموعة من المستخدمين بشكل سريع وآمن، كما وتقلل النفقات، كما وتعمل على تطوير جميع أنواع الاتصالات وتبادل البيانات[2].

اما بالنسبة للخصائص البيولوجية فيتميز كل انسان عن غيره بسمات بيولوجية لا يشترك بها مع أحد، مما دعا شركات الأمن المعلوماتي، إلى تطوير أجهزة تعمل على الخصائص البيولوجية للإنسان، والتي لا تسمح بالوصول إلى النظام المعلوماتي الا لأشخاص مصرح لهم بذلك ومن هذه الأجهزة، أجهزة استخدام بصمة الابهام، وبصمة الصوت، وحدقة العين، وبصمة خط اليد[3].

نخلص مما تقدم أن هنالك برامج وطرق ونظم من الضروري الاستعانة بها للحفاظ على البيانات أو المعلومات أو البرامج أو الانظمة الالكترونية أو الشبكات.. الخ، كما أرى من المناسب أدراج نص قانوني في مشروع قانون الجرائم المعلوماتية، يشترط أن يكون تصنيع نظم الحماية وكذلك البرامج أو الحاسبات وغيرها من التقنيات المستخدمة داخل المؤسسات الحكومية في العراق، أو من قبل دولة حليفة

(1) محمد امين الرومي، مرجع سابق، ص210.

(2) د. ايمن عبد الحفيظ عبد الحميد سلمان، مرجع سابق، ص400.

(3) للمزيد عن هذة الاجهزة: نهلا عبد القادر المومني، مرجع سابق، ص 220. د. ايمن عبد الحفيظ عبد الحميد سلمان، مرجع سابق، ص391 وما بعدها. منير محمد الجهني وممدوح محمد الجهني، الشركات الالكترونية، مرجع سابق، ص 140 - 141. ممدوح الشيخ= =، التجسس التكنولوجي سرقة الاسرار الاقتصادية والتقنية، مكتبة بيروت، مسقط، 2007، ص 150.

للعراق، خاصة بعد أن عرفنا من خلال ماتقدم دراسته، قيام بعض شركات تصنيع البرامج من وضع برامج تجسسية، خاصة وأن العراق متجه نحو إدخال التقنية في كل مجالات وخاصة الأمنية والسياسية والعسكرية.

ونقترح أن يكون النص بالصيغة الاتية "يستخدم داخل المؤسسات الحكومية وشبه الحكومية، نظم معلوماتية وبرامج حماية للبيانات أو المعلومات وغيرها من الوسائل التقنية مصنعة في العراق، أو من مناشئ رصينة تخضع لفحص وأشراف كادر من المهندسين العراقيين المختصين، لبيان مدى الأمان الذي توفره هذه النظم المعلوماتية أو التقنية للبيانات أو المعلومات والبرامج وغيرها المخزنة في داخلها أو التي ترسل عن طريقها عبر الموجات الكهربائية".

الفصل الثاني

ماهية جريمة التجسس المعلوماتي

عرف العالم التجسس منذ أقدم العصور ومنذ نشوء الدولة بالمفهوم القديم والحديث، وارتبط التجسس بالحرب والذي عد بمثابة سلاح سري لمباغتة العدو والذي أدى في بعض الحالات إلى تقرير مصير دول ومعارك مهمة [1].

وفي عهد الاسلام نهى القرآن الكريم عن تجسس المسلمين بعضهم على بعض، حفاظا وصيانة لحرمة الحياة الخاصة، في قولة تعالى: ﴿وَلَا تَجَسَّسُوا وَلَا يَغْتَبْ بَعْضُكُمْ بَعْضاً أَيُحِبُّ أَحَدُكُمْ أَنْ يَأْكُلَ لَحْمَ أَخِيهِ مَيْتاً فَكَرِهْتُمُوهُ وَاتَّقُوا اللَّهَ إِنَّ اللَّهَ تَوَّابٌ رَحِيمٌ﴾ [2]. فهو من الافعال المذمومة، ولكن ليس كل تجسس مذموم، إذ إن التجسس على الاعداء من عوامل الظفر بهم، ويحظى المتجسس بالاحترام والتقدير[3].

(1) قحطان محمد صالح الجميلي، الباحثون عن الاسرار، منشورات مكتبة الدار القوقية، بغداد، 1986، ص 11 ومابعدها.

(2) سورة الحجرات، من الاية (12).

(3) هاني رفيق حامد عوض، الجريمة السياسية ضد الافراد، رسالة ماجستير، الجامعة الاسلامية كلية الشريعة والقانون، غزة، 2009، ص 85. محمد راكان الدغمي، التجسس واحكامة في الشريعة الاسلامية، ط 3، دار السلام، القاهرة، 2006، ص 31.

أما القوانين الوضعية فقد جرمت فعل التجسس، ونظمت أحكام هذة الجريمة التقليدية التي تتطلب الدخول المادي للشخص للمواقع السرية، كما تتطلب العمل على تدريب الجاسوس[1].

وبعد الثورة العلمية التي شهدها العالم ودخول الحاسوب في شتى المجالات، ووجود طائرات التجسس والاقمار الصناعية[2] والبث الفضائي علاوة على شبكة الانترنت اصبحت حدود الدول مستباحة، مما أبرز شكلا جديداً للتجسس ألا وهو التجسس المعلوماتي، حيث عمدت الدول إلى وضع أجهزة متخصصة بالعمل الاستخباري تمارس أعمال التجسس[3].

وتأسيسا على ما تقدم سنتناول في هذا الفصل تحديد مفهوم جريمة التجسس المعلوماتي وطبيعتها ونطاقها وذلك في مبحثين:

- **نخصص المبحث الأول** لمفهوم جريمة التجسس المعلوماتي.
- **ونفرد المبحث الثاني** لطبيعة جريمة التجسس المعلوماتي ونطاقها.

(1) لم يقتصر عمل التجسس على الذكور بل عملت بعض النساء بالتجسس وكان لها دورا مهما في التجسس ونقل المعلومات يوازي دور الرجال، كما في الحرب الاهلية الامريكية، للمزيد ينظر: د. رحيم كاظم الهاشمي و د. علي خوير مطرود، التجسس في الحرب الاهلية الامريكية= =(1861 - 1865)، مجلة الاستاذ، كلية التربية أبن رشد الانسانية – جامعة بغداد، المجلد الاول، العدد 250، 2013، ص 469.

(2) فقد سبق أستخدام طائرات التجسس والاقمار الصناعية، استخدام المناطيد للتجسس من قبل الفرنسيين، وكانت اول صورة فوتوغرافية التقطت بالمنطاد كان عام 1858 من قبل (كاسبرد فيلكس) وهو عسكري في جيش نابليون. ينظر: د. رحيم كاظم الهاشمي و د. علي خوير مطرود، مرجع سابق، ص 469. برهام يوست، ترجمة علي جواد حسين، ط1، الدار العربية للموسوعات، بيروت، 1999، ص 17 ومابعدها.

(3) تمارس الولايات المتحدة الامريكية التجسس الالكتروني بشكل منظم على أغلب الدول، من خلال عملاء لها من اجهزة المخابرات للدول الاخرى، حيث تقوم وكالة (CIA) بالتنصت على جميع الاتصالات التي تجري في العالم، وبالتعاون مع دول أقليمية هي كندا وبرطانيا واستراليا ونيوزلندا تعمل على رصد المكالمات الهاتفية والرسائل ما كان منها، برقيا، فاكسيا، الكترونيا، تلكسيا. للمزيد ينظر: محمد خليل الحكايمة، أسطورة الوهم، بدون دار نشر، 2011، ص8. متاح على الموقع www.almajd.ps/upload/books/wahm.وقت وتاريخ الزيارة: 2300، 3/8/ 2015. د. عبد الرحمن جلهم حمزة، مرجع سابق، ص 98 - 99.

المبحث الاول

مفهوم جريمة التجسس المعلوماتي

أتسع مفهوم التجسس المعلوماتي ليشمل أغلب الأفعال التي تمس مؤسسات الدولة والشركات والمنظمات والحياة الخاصة....الخ، وتمثلت هذة الأفعال بالدخول غير المشروع أو اعتراض المعلومات[1]، أو التنصت عليها أو الالتقاط لها، وأن الغرض من الدخول للنظام المعلوماتي انتهاك سرية البيانات سواء كانت سياسية أو اقتصادية...الخ.

وبناءً على ماتقدم سنتولى تحديد مفهوم جريمة التجسس المعلوماتي من خلال تعريفها وبيان ذاتيتها وذلك في مطلبين.

(1) د. عبد الفتاح بيومي حجازي، الجرائم المستحدثة....، مرجع سابق، ص252 - 253.

المطلب الاول

تعريف جريمة التجسس المعلوماتي وذاتيتها

- **سنتناول في الفرع الأول:** منه تعريف جريمة التجسس المعلوماتي لغة واصطلاح.
- **ويخصص الفرع الثاني:** لذاتية جريمة التجسس المعلوماتي.

الفرع الاول

تعريف جريمة التجسس المعلوماتي

أولا: تعريف جريمة[1] التجسس المعلوماتي[2] لغة:

جس جسست، يجس، اجسس، جس، جسا، فهو جاسوس والمفعول مجسوس[3]، والجس هو جس الخبر، وتجسسه بحث عنه[4]، أي تفحصه، ومنه الجاسوس[5]، وجس الشخص بعينه أحد النظر اليه ليستبينه[6]، والتجسس بالجيم التفتيش عن بواطن الأمور، والجاسوس هو صاحب سر الشر[7]، وهو العين الذي يتجسس الأخبار[8].

ثانيا: تعريف جريمة التجسس المعلوماتي اصطلاحا:

قانونا نجد إن التشريع العراقي قد تناول جريمة التجسس بصورتها التقليدية، إلا أنه لم يعرف التجسس، بل اكتفى بتحديد الافعال، التي يعتبر مرتكبها جاسوسا، وذلك بالنص عليها في قانون العقوبات العراقي رقم 111 لسنة 1969[9]، والذي لم يطلق عليها لفظ التجسس كما سنبينه عند تناول

(1) المعنى اللغوي للجريمة ينظر ص (7) من الرسالة.

(2) المعنى اللغوي للمعلوماتية ينظر ص (7) من الرسالة.

(3) د. أحمد مختار عمر، معجم اللغة العربية المعاصرة، ط 1، عالم الكتاب، القاهرة، 2008، ص 374.

(4) محمد بن مكرم بن منظور الافريقي المصري، لسان العرب، ج 6، دار صادر، بيروت، 1997، ص 38.

(5) محمد بن ابي بكر عبد القادر الرازي، مختار الصحاح، مكتبة لبنان، بيروت، 1986، 2010، ص 44.

(6) الحسن بن محمد بن الحسن الصاغني، العباب الزاخر واللباب الفاخر، تحقيق محمد حسن ال ياسين، ، ج 1، دار الرشيد للنشر، بغداد، 1981، ص 76.

(7) خياط يوسف، لسان العرب المحيط، دار لسان العرب، بيروت، 1960، ص 38.

(8) محمد مرتضى الحسيني، تاج العروس من جواهر القاموس، تحقيق مصطفى حجازي، ج 17، المطبعة الحكومية، الكويت، 1977، ص 6.

(9) المواد (158، 159، 164، 177) قانون العقوبات العراقي رقم 111 لسنة 1969.

أساس التجريم على المستوى الوطني، ومن الجدير بالذكر لم يحددالمشرع العراقي الوسيلة المستخدمة للحصول على المعلومات المحظورة و نشرها أو اذاعتها[1]، ومن ثم يمكن أن يكون الحصول على المعلومات السرية بطريقة الكترونية، أما مشروع قانون الجرائم المعلوماتية العراقي لعام 2012 فكذلك لم يتضمن تعريفاً للتجسس المعلوماتي، والذي تناول تجريم صور التجسس المعلوماتي، كالدخول أو البقاء غير المشروع، جريمة الاعتراض غير المشروع، جريمة تهديد أمن الدولة، جريمة الاعتداء على سلامة البيانات، جرائم الاعتداء على حرمة الحياة الخاصة، إفشاء معلومات أو اسرار المشتركين[2].

ويقصد بالتجسس التقليدي في التشريع الجنائي الفرنسي بأنه(السعي للحصول على الاخبار أو الوثائق السرية أو الخرائط العسكرية دون سبب قانوني أو أذن الجهة المسؤولة، وتسليمها إلى دولة أجنبية، أو افشاء الأسرار الاقتصادية عمدا)[3].

في حين جاءت (الفقرة 4 من المادة 411) من قانون العقوبات الفرنسي لعام 1992 المعدل لتضع المبادئ الأساسية التي تسهم في إمكانية وضع تعريف للتجسس الدولي[4]، حيث نصت على أن "كل فعل يقوم به أجنبي ويؤدي إلى الاضرار بالمصالح الأساسية للأمة والدولة، والتي تتألف من أمنها وأستقلالها وسلامتها الاقليمية، وشكل نظامها الجمهوري، ومؤسساتها ووسائل دفاعها، وعلاقاتها الدوبلوماسية، وحماية الشعب داخل وخارج فرنسا وتوازنه في وسطه

(1) المادة (182) قانون العقوبات العراقي.

(2) المواد (3، 4، 5، 6، 7، 14، الفقرة د من المادة 19) من مشروع قانون الجرائم المعلوماتية العراقي.

(3) قانون العقوبات الفرنسي الصادر عام 1934 الملغي. منتظر سعيد حمودة، الجريمة السياسية، دار الفكر الجامعي، الاسكندرية، 2009، ص 128. د.علي يوسف الشكري، الاتجاهات الحديثة في تحديد مسؤولية رئيس الدولة في فرنسا. مجلة الكوفة للعلوم القانونية والسياسية، كلية القانون- جامعة الكوفة، المجلد 1، العدد 5، 2010، ص 9.

(4) د. محمود سليمان موسى، التجسس الدولي والحماية الجنائية للدفاع الوطني وأمن الدولة، مشأة المعارف، الاسكندرية، 2001، ص 116.

الطبيعي ومحيطة، والعناصر الأساسية في مقدراتها العلمية والاقتصادية وتراثها الحضاري".

أما عن تعريف التجسس المعلوماتي، فعلى الرغم من تناوله بصورته الالكترونية في القوانين المقارنة، لم أجد تعريفا له كما لم يطلق عليه لفظ التجسس أيضا، فأطلق القانون الفرنسي لفظ كل فعل تسليم أو اتاحة الحصول إلى أي قوة أجنبية...على معطيات رقمية الكترونية....الخ[1] أو لفظ الدخول أو البقاء غير المشروع[2] أو الالتقاط أو التنصت..الخ[3]. وأطلق القانون الأمريكي، لفظ الدخول العمدي بدون تصريح أو تجاوز التصريح، كما أستخدمت عبارة الوصول عمدا بدون ترخيص أو تجاوز الترخيص[4]. و اطلق النظام السعودي على التجسس لفظ التنصت أو الالتقاط أو الاعتراض أو الدخول غير المشروع للنظام المعلوماتي[5]. أما القانون الاماراتي أطلق لفظ الدخول دون تصريح أو بتجاوز التصريح، كذلك الاعتراض أو الالتقاط...الخ[6].

فقها يعرف التجسس المعلوماتي بأنه:(استخدام وسائل تقنية المعلومات الحديثة للدخول بشكل غير مسموح وغير قانوني، إلى أنظمة المعلومات الالكترونية الخاصة بالدولة والحكومات والتنصت عليها، بقصد الاستحصال على ما لديها من معلومات مهمة تتعلق بنظامها وأسرارها، وتشمل جميع أنواع المعلومات العسكرية والسياسية والامنية والاقتصادية والعلمية والاجتماعية)[7].

---

(1) المادة (411) من قانون العقوبات الفرنسي المتعلق بالجرائم ضد الامة رقم 913 - 93 لعام 1993. للمزيد: د.علي جعفر، مرجع سابق، ص 574.

(2) ينظر: (الفقرة 1 من المادة 323) من قانون العقوبات الفرنسي الجديد لعام 1992 المعدل.

(3) ينظر: (الفقرة 1 من المادة 226) من قانون العقوبات الفرنسي الجديد.

(4) المادة (1030/أ/2) من القانون الفدرالي الاتحادي الخاص بأساءة استخدام الحاسوب رقم (18) لسنة 1984 المعدل في عام 1996.

(5) المادة (3) والمادة (7) من النظام السعودي لمكافة الجريمة المعلوماتية.

(6) ينظر: المواد (2،4،12،15،21،22) من مرسوم رقم (5) لعام 2012 لمكافحة جرائم تقنية المعلومات الاماراتي.

(7) د.علي جعفر، مرجع سابق، ص 569.

ويعرف أيضا بأنه: القيام بجمع المعلومات والوثائق السرية، التي تخص الأمور العسكرية أو السياسية أو الاقتصادية بقصد تسليمها إلى دولة أجنبية، بمقابل أو بدون مقابل، وذلك بأختراق الانظمة المعلوماتية أو الشبكات المعلوماتية أو اعتراض الاتصالات(1).

ويعرف أيضا بأنه(استراق السمع أو البصر للتجسس سواء باستخدام الأذن أو النظر أو استخدام أجهزة متخصصة في ذلك)(2).

أما الجاسوس فهو (العين الذي يرسل بين العدو ليراقب ويستطلع وينقل الأخبار).

ويعرف أيضا بأنه (الشخص الذي يطلع على عورات المسلمين ليكشفها للعدو)(3).

أما تعريف التجسس المعلوماتي قضاءً لم يعرف القضاء التجسس المعلوماتي - طبقا لما اطلعنا عليه من قرارات - .

وعرف التجسس التقليدي في قرار لمحكمة النقض المصرية بأنه (هو تسليم سر من أسرار الدفاع إلى دولة أجنبية أو من يعمل لمصلحتها، أو الحصول عليه بغض النظر عن الوسيلة المستعملة، ويكون ذات طبيعة سرية ومتعلق بالدفاع عن البلاد، وإن لم يفش إلا بعضه أو كان خطأ أو ناقصا)(4).

(1) منى فتحي احمد عبد الكريم، مرجع سابق، ص 111 - 112.

(2) خالد بن غنام الفريدي الحربي، التنصت بين الشريعة والقانون، رسالة ماجستير، جامعة نايف العربية للعلوم الامنية، 2012، ص 28.

(3) محمد راكان الدمغي، مرجع سابق، ص 28 - 29.

(4) ينظر: الطعن رقم 1519 ق جلسة 13 /1958/5 محكمة النقض المصرية. أشار اليه: حسن الفكهاني وعبد المنعم حسني، الموسوعة الذهبية للقواعد القانونية التي قررتها محكمة النقض المصرية منذ إنشاءها 1931، ج 3، الدار العربية للموسوعات، القاهرة، 1982، ص 46 - 47.

وتأسيسا على ماتقدم يمكن تعريف جريمة التجسس المعلوماتي بأنها: (الدخول غير المصرح به أو تجاوز التصريح الممنوح، إلى نظام معلوماتي أو موقعا الكترونياً أو شبكة معلوماتية، أو أية وسيلة تقنية أخرى، باستخدام الشبكة المعلوماتية أو الحاسب الآلي أو أحدى الوسائل التقنية، لانتهاك سرية البيانات الحكومية أو الخاصة، بالاطلاع عليها أو نسخها أو نشرها أو اذاعتها أو أفشائها أو كشفها أو تسليمها الى الغير(دولة، شركات، فرد..الخ)، بمقابل أو بدون مقابل).

الفرع الثاني

ذاتية جريمة التجسس المعلوماتي

أولا: جريمة التجسس المعلوماتي وجريمة الارهاب المعلوماتي.

1 - تعريف الارهاب المعلوماتي:

(استخدام التقنيات الرقمية لأخافة واخضاع الاخرين، أو مهاجمة نظم المعلومات بدوافع سياسية أو اقتصادية أو امنية أو عرقية أو دينية)(1).

ويعرف أيضا بأنه (العدوان أو التخويف أو التهديد ماديا أو معنويا باستخدام الوسائل الالكترونية الصادرة من الدول أو الجماعات أو الأفراد، على الإنسان في دينه، أو نفسه أو عرضه، أو ماله، أو عقله، بغير حق بشتى صنوف وصور الإفساد في الأرض)(2).

تتشابه الجريمتان من حيث أنهما يمثلان أنتهاكا لحقوق خصها المشرع الجنائي بالحماية، وأن كلاهما يرتكبان بتقنية المعلومات، ولا يحتاجان إلى استخدام العنف في ارتكابهما، وهما من الجرائم العابرة للحدود(3)، كما تتسمان بصعوبة الاكتشاف والاثبات، كما أن فعل التجسس من صور الركن المادي

(1) بهاء فهمي الكبيجي، مدى توافق احكام جرائم أنظمة المعلومات في القانون الاردني مع الاحكام العامة للجريمة، رسالة ماجستير، جامعة الشرق الاوسط، 2013، ص 85.

(2) د. ايسر محمد عطية، دور الاليات الحديثة للحد من الجرائم المستحدثة الارهاب الالكتروني وطرق مواجهته، ورقة علمية مقدمة الى الملتقى العلمي (الجرائم المستحدثة في ظل المتغيرات والتحولات الاقليمية والدولية)، كلية العلوم الاستراتيجية، عمان، 2014، ص 8.

(3) زين العابدين عواد كاظم الكردي، جرائم الارهاب المعلوماتي و بعض تطبيقاتة في القانون العراقي، رسالة ماجستير، جامعة بابل كلية القانون، 2008، ص 65.

للجريمتين[1]، علاوة على أن الجاني في الجريمتين قد يكون دولة أو عدة دول أو أفراد أو جماعات[2]، كما يشتركان في وحدة المجني عليه حيث إن المجني عليه هو المؤسسات العسكرية والسياسية والاقتصادية...الخ[3]، يضاف إلى ذلك تستخدم الجريمتين الفيروسات وغيرها من البرامج الضارة في تنفيذ الأعمال الإجرامية، مثل اختراق البريد الالكتروني بواسطة الفيروس[4]، كما أن الجريمتين لا تحتاج في ارتكابهما إلى العنف والتطرف[5].

وتختلف الجريمتان في أن جريمة التجسس المعلوماتي تستهدف المعلومات السرية، أما جريمة الارهاب المعلوماتي ليس بالضرورة أن تستهدف المعلومات السرية[6]، كما لا تعتبر جرائم الإرهاب من الجرائم الماسه بالحرية الشخصية[7]،

---

(1) د. طارق عبد العزيز حمدي، المسؤولية الدولية والجنائية والمدنية عن جرائم الارهاب الدولي، ط 1، دار الكتب القانونية، القاهرة، 2008، ص 308 وما بعدها. وائل أبراهيم مصلحي، الجرائم المستحدثة في ظل المتغيرات والتحولات الاقليمية والدولية، ورقة علمية مقدمة الى الملتقى العلمي (الجهود الوطنية لمواجهة الجرائم المستحدثة)، كلية العلوم الاستراتيجية، الاردن، 2014. حسن طاهر داود، جرائم نظم...، مرجع سابق، ص 76.

(2) هيثم فالح شهاب، جريمة الارهاب وسبل مكافحتها، ط 1، دار الثقافة، عمان، 2010، ص 54 وما بعدها. د. طارق عبد العزيز حمدي، المسؤولية الدولية والجنائية والمدنية عن جرائم الارهاب الدولي، دار الكتب القانونية، مصر، 2008، ص 306. د.يوسف بن احمد الرميح، الارهاب والجريمة الالكترونية بالمجتمع السعودي رؤية سوسيولوجية، مجلة كلية الاداب، جامعة جنوب الوادي – مصر، العدد 27، 2009، ص 224. عطا بن ناصر بن سعيد العطوي، الارهاب المنظم في المجتمع الدولي، رسالة ماجستير، جامعة نايف العربية للعلوم الامنية – كلية العدالة الجنائية، الرياض، 2015، ص 79 ومابعدها. د. عادل عبد الجواد محمد الكردوسي، مرجع سابق، ص 123.

(3) د. حسين المحمد بوادي، مرجع سابق، ص 104. د. محمود سامي الشوا، مرجع سابق، ص 68 - 69.

(4) د. أيسر محمد عطية، مرجع سابق، ص 11.

(5) بهاء فهمي الكبيجي، مرجع سابق، ص 86.

(6) د. سعد ابراهيم الاعظمي، جرائم التعاون مع العدو في زمن الحرب /دراسة مقارنة، القانون والسياسة، بغداد، 1984، ص 50.

(7) د. أشرف توفيق شمس الدين، الحماية الجنائية للحرية الشخصية من الوجهة الموضوعية ((دراسة مقارنة))، ط2، دار النهضة العربية، القاهرة، 2007، ص 58.

في حين تعتبر جريمة التجسس ماسه بالحياة الخاصة، أضافة إلى أن المتجسسين يعملون بالخفاء[1]، أما الأعمال الإرهابيه فإن الصفه الغالبة هي عملهم بالعلن، يضاف إلى ذلك أن جريمة الارهاب تعتبر من جرائم أمن الدولة الداخلي[2]، أما جريمة التجسس المعلوماتي فهي من جرائم أمن الدولة الخارجي[3]، علاوة على ذلك يستخدم مجرمو الارهاب المعلوماتي البريد الالكتروني للترويج لأفكاررهم الهدامة[4]، وهو أمر غير موجود في جريمة التجسس المعلوماتي، كما تختلف جريمة الارهاب المعلوماتي عن التجسس المعلوماتي باستخدامها مواقع المؤسسات والشركات والجهات الرسيمة والافراد[5] ومواقع المنتديات البعيدة عن الشبهة لتبادل المعلومات للمواقع المستهدفة[6].

ثانيا: جريمة التجسس المعلوماتي وجريمة القرصنة الالكترونية.

يقصد بالقرصنة الالكترونية بأنها:(عملية اختراق لأجهزة الكومبيوتر عن طريق شبكة الانترنت غالبا، وذلك لارتباط الحواسيب حول العالم بشبكة الانترنت أو شبكات داخلية، يقوم بها شخص أو عدة اشخاص لديهم خبرة في مجال البرمجيات، للقيام بسرقة المعلومات من البرامج أو النسخ غير المشروع للبرامج)[7].

(1) قحطان محمد صالح الجميلي، مرجع سابق، ص 15.
(2) د. أيمن عبد الحفيظ، مرجع سابق، ص 171.
(3) د. علي جعفر، مرجع سابق، ص 569.
(4) د. فايز بن عبد الله الشهري وآخرون، استعمال الانترنت في تمويل الارهاب وتجنيد الارهاب، ط 1، جامعة نايف العربية للعلوم الامنية، الرياض، 2012، ص 22.
(5) د. فايز بن عبد الله الشهري وآخرون، مرجع سابق، ص 53.
(6) د. فايز بن عبد الله الشهري وآخرون، مرجع نفسه، ص 22.
(7) د. عماد مجدي عبد الملك، مرجع سابق، ص 84. محمود أحمد عبابنة، مرجع سابق، ص 93.

من أوجه الشبه بين الجريمتين أنهما يشكلان انتهاكا للقواعد القانونية، واعتداءاً على المصالح التي هي جديرة بالحماية بنظر المشرع، ومن بين هذه المصالح على سبيل المثال الاعتداء على الملكية الفكرية[1]، وعلى الاسرار الصناعية والتجارية...الخ[2]، كما أن محل الجريمتين قد يكون الاشخاص أو الحكومات أو الشركات....الخ، وقد يكون الدافع في كلا الجريمتين سياسيا[3]، علاوة على أن الجريمتين عابرة للحدود[4]، كما تمثلان عقبة امام مستخدمي النظام الشرعين، إذ تمنعهم من الوصول إلى البيانات الموجودة داخل النظام المعلوماتي وذلك بحجبهم و استغلال المواقع نفسها أو إنشاء مواقع وهمية تشبه المواقع الأصلية[5]، كما تساعد الجريمتين على انتشار الفيروسات داخل النظام المعلوماتي[6] وتهدف

(1) د. حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الانترنت، دار النهضة العربية، القاهرة، 2009، ص 313.

(2) د. بركات محمد مراد، القرصنة الدولية وحقوق الملكية الفكرية، مجلة المحيط الثقافي، تصدرها وزارة الثقافة المصرية، العدد 25، 2002، ص 2. د. باقر عطية هويدي الخيكاني، الجرائم المعلوماتية وتأثيرها في المجتمع، دار الفرات للثقافة والاعلام، الحلة، 2013، ص 141. د. سليمان أحمد فضل، مرجع سابق، ص 385 - 386.

(3) زياد خلف عبد الله الجبوري و محمد شطب عيدان المجمعي، القرصنة التكنولوجية واثرها في العلاقة الامريكية – الصينية، مجلة جامعة تكريت للعلوم الانسانية، العدد 9، 2008، ص 431. د. نعيم مغبغب، مخاطر المعلومات والانترنت المخاطر على الحياة الخاصة وحمايتها دراسة في القانون المقارن، ط2، منشورات الحلبي الحقوقية، بيروت، 2008، ص 193 - 194. د. حسين المحمدي بوادي، مرجع سابق، ص 69.

(4) د. عبد الفتاح بيومي حجازي، الجواب الاجرائية لاعمال التحقيق...، مرجع سابق، ص 72.

(5) د. هلالي عبد اللاه احمد، أتفاقية بودابست لمكافحة جرائم المعلومات معلقا عليها، ط1، دار النهضة العربية، القاهرة، 2007، ص 50 ومابعدها. د. عبد الفتاح بيومي حجازي، الحكومة الاكترونية بين الواقع والطموح، مرجع سابق، ص 511 - 512.

(6) في هذا المعنى ينظر: زياد خلف عبد الله الجبوري و محمد شطب عيدان المجمعي، مرجع سابق، ص 431. د. حسين الغافري و محمد الالفي، جرائم الانترنت بين الشريعة الاسلامية والقانون، دار النهضة العربية، القاهرة، 2008، ص 161. د. خالد ممدوح ابراهيم، فن التحقيق....، مرجع سابق، ص 442. د. نائلة محمد قورة، جرائم الحاسب الالي الاقتصادية، مرجع سابق، ص 296.

الجريمتان إلى ادخال برامج تجسسية الى حواسيب الضحايا[1]، كما تتشابه الجرمتين بوسائل ارتكابهما وذلك بالالتقاط الذهني للبيانات بالنظر والاستماع، بالتقاط الموجات التي يرسلها الكومبيوتر عند تشغيله[2] أو باعتراض معطيات الحواسيب خلال عملية نقلها، أو باختراق النظم المعلوماتية[3].

أما أوجه الاختلاف فالقرصنة في الغالب هي من جرائم الاعتداء على الملكية الفكرية، أما جريمة التجسس المعلوماتي فهي أكثر شمولا إذ تستهدف اغلب المؤسسات العامة والخاصة بالدولة، يضاف الى ذلك ان الدافع في جريمة القرصنة الالكترونية يكون باستعراض قدرات الجاني التقنية[4] أو الشهوة أو الربح[5]، أما الدافع لارتكاب جريمة التجسس المعلوماتي هو التلصلص او انتهاك سرية البيانات في الغالب[6]، كما تختلف جريمة القرصنة في أن القراصنة يتطلعون إلى المغامرة وذلك باكتشاف طرق وأساليب جديدة للحصول على المعلومات و يرون أن جميع المعلومات يجب ألا تكون خاضعة للقيود [7].

(1) د. عماد مجدي عبد الملك، مرجع سابق، ص 126.

(2) محمود احمد عبابنة، مرجع سابق، ص 94. د. خالد ممدوح ابراهيم، فن التحقيق.....، مرجع سابق، ص 445. د. نعيم مغبغب، مخاطر المعلومات...، مرجع سابق، ص 181.

(3) د. عمر ابو الفتوح عبد العظيم الحمامي، مرجع سابق، 221. محمود احمد عبابنة، مرجع سابق، ص 94. د. عبد الفتاح بيومي حجازي، الجرائم المستحدثة....، مرجع سابق، ص 191 - 192.

(4) د. نائلة عادل محمد فريد قورة، مرجع سابق، ص 38.

(5) د. خالد ممدوح ابراهيم، الجرائم المعلوماتية، مرجع سابق، ص 145.

(6) د. عبد الفتاح بيومي حجازي، الاحداث والانترنت، مرجع سابق، ص 229.

(7) د. طارق ابراهيم الدسوقي عطية، الامن المعلوماتي (النظام القانوني لحماية المعلومات)، دار الجامعة الجديدة، الاسكندرية، 2009، ص 548. د. حسين الغافري و محمد الالفي، مرجع سابق، ص 45 - 46.

المطلب الثاني

أساس تجريم التجسس المعلوماتي

سنتناول في هذا المطلب أساس تجريم التجسس المعلوماتي على الصعيد الدولي والوطني، وذلك في فرعين وعلى النحو الآتي.

- **الفرع الاول:** أساس تجريم التجسس المعلوماتي على الصعيد الدولي.
- **الفرع الثاني:** أساس تجريم التجسس المعلوماتي على الصعيد الوطني.

الفرع الاول

أساس تجريم التجسس المعلوماتي على الصعيد الدولي

عرفت المادة (29) من اتفاقية لاهاي الرابعة لعام 1907 الجاسوس بأنه " الشخص الذي يعمل بالخفاء أو تحت ستارٍ كاذب، لجمع المعلومات أو محاولة ذلك في منطقة العمليات الحربية، بغية إيصالها للدولة المعادية الاخرى"، من الجدير بالذكر أن اتفاقية لاهاي قد حصرت معنى الجاسوس على الأجنبي دون الوطني وذلك لخضوع المواطن للقانون الوطني[1]، كما تنطبق أحكامها على التجسس في منطقة العمليات الحربية للأطراف المتنازعة، وهو ما لا يدع مجالاً لتطبيق الاتفاقية على التجسس الذي يتم في حالة السلم[2].

وحضر الأعلان العالمي لحقوق الانسان لعام 1948 أي اعتداء على حرمة الحياة الخاصة أو على سرية المراسلات وذلك في المادة (12) حيث نصت على أنه "يحظر تعريض الفرد لتدخلات تحكمية في حياته الخاصة، أو أسرته أو مسكنه أو مراسلاته.....".

وقد أكدت الاتفاقية الاوربية لحقوق الانسان لعام 1950 في المادة (8) منها على حرمة الحياة الخاصة وحرمة المراسلات الشخصية إذ نصت على أن" لكل إنسان حق احترام حياته الخاصة والعائلية ومسكنه ومراسلاته".

(1) قحطان محمد صالح الجميلي، مرجع سابق، ص 13.

(2) د. محمود سليمان موسى، مرجع سابق، ص 13 هامش رقم (1).

كما حظرت المادة (17) من الاتفاقية الدولية للحقوق المدنية والسياسية لعام 1966، اي تدخل تعسفي أو غير قانوني في الحياة الخاصة للفرد أو أسرته وأكدت على حماية مسكنه وسريه مراسلاته إذ نصت " لا يجوز التدخل بشكل تعسفي أو غير قانوني في خصوصيات أحد أو بعائلته أو بيته أو مراسلاته...، ولكل شخص الحق في حماية القانون ضد مثل هذا التدخل أو التعرض".

وعرفت المادة 46 من برتكول عام 1977 الملحق باتفاقية جنيف لعام 1949، الجاسوس بأنه " ذلك الذي يجمع او يحاول ان يجمع معلومات عسكرية في الخفاء أو باستخدام الغش والخداع".

أما عن اتفاقية بودابست لعام 2001 فقد جرمت الاعتراض غير القانوني حيث نصت في المادة (3) على أن "على كل طرف أن يتبنى الاجراءات التشريعية أو أي اجراءات أخرى يرى أنها ضرورية من أجل اعتبارها جريمة جنائية، وفقا لقانونها الداخلي واقعة الاعتراض العمدي وبدون حق، من خلال وسائل فنية للارسال غير العلني لبيانات الحاسب في مكان الوصول في المنشأ، أو في داخل النظام المعلوماتي، بما في ذلك الانبعاثات الكهرومغناطيسية من جهاز حاسب يحمل هذة البيانات، كما يمكن لأي طرف أن يستوجب أن ترتكب الجريمة بنية إجرامية (بقصد الغش)، أو أن ترتكب الجريمة في حاسب آلي، يكون متصلا عن بعد بحاسب آخر"، ومن الجدير بالذكر أن صفة غير العلنية المذكورة بالاتفاقية تتبع وسيلة الاتصال أو النقل وليس طبيعة البيانات المرسلة[1]، يلاحظ على النص أنه جرم التجسس والتنصت على المعلومات والبيانات، والذي يتم بشكل مباشر عن طرق الدخول للنظام المعلوماتي، أو بشكل غير مباشر أما باعتراض الانبعاثات الكهرومغناطيسية، أو باستخدام الوسائل الفنية للتنصت، أو يتم، و منح النص المتقدم الدول الاطراف حرية جعل تجريم الافعال المتقدمة تتم بقصد أو دون قصد، أي تجريم مجرد الدخول أو التنصت، أو جعل ذلك بقصد تحقيق غاية معينة.

(1) د. هلالي عبد اللاه احمد، مرجع سابق، ص 63.

أنتقد استخدام اتفاقية بودابست عبارة الاعتراض غير القانوني للدلالة على صور التجسس الأخرى وهي الدخول غير المشروع أو الالتقاط أو التنصت المعلوماتي، وذلك لأن أفعال الاعتراض غير القانوني والدخول غير المشروع أو الالتقاط أو التنصت تشكل جرائم مستقلة كما ذهبت أغلب تشريعات الدول إلى ذلك كالفرنسي والامارتي والسعودي ومشروع قانون الجرائم المعلوماتية العراقي... الخ.

أما عن الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010 فقد جرمت الدخول غير المشروع أو البقاء، وكل اتصال غير مشروع مع كل أو جزء من تقنية المعلومات أو الاستمرار به، و تشدد العقوبة إذا ترتب على الدخول أو البقاء أو الاتصال أو الاستمرار بهذا الاتصال، الحصول على معلومات حكومية سرية.

وذلك في المادة (6) منها حيث نصت على أن "جريمة الدخول غير المشروع: 1 - الدخول أو البقاء وكل أستعمال غير مشروع مع كل أو جزء من تقنية المعلومات أو الاستمرار به. 2 - تشدد العقوبه إذا ترتب على الدخول أو البقاء أو الاتصال أو الاستمرار بهذا الاتصال: أ - محو أو تعديل أو نسخ أو نقل أو تدمير للبيانات المحفوظة والأجهزة والأنظمة الألكترونية وشبكات الإتصال وإلحاق الضرر بالمستخدمين والمستفيدين. ب - الحصول على معلومات حكومية سرية".

كما جرمت المادة (7) من الاتفاقية ذاتها الاعتراض غير المشروع إذ نصت على أن "الاعتراض المتعمد بدون وجه حق، لخط سير البيانات بأي من الوسائل الفنية، وقطع بث أو استقبال بيانات تقنية المعلومات"، حيث أن هذة المادة تجرم صورة من صور التجسس، وهي اعتراض البيانات، بعد أن تناولت بالتجريم الدخول أو البقاء أو الاتصال أو استمرار الاتصال غير المشروع، من خلال استعراض نصوص اتفاقية بودابست والاتفاقية العربية نجد أن الاتفاقية العربية كانت أكثر وضوحا من اتفاقية بودابست، والتي جرمت فقط فعل الاعتراض لسير البيانات،

إذ يتطلب الأمر الرجوع إلى المذكرة التفسيرية لمعرفة المقصود بالاعتراض والتي بينت أن الاعتراض يتم بالوسائل الفنية، والذي يتم بشكل مباشر بالدخول إلى النظام المعوماتي، أو بشكل غير مباشر بالتنصت عليها[1]، أما الاتفاقية العربية فقد جرمت صراحة الدخول أو البقاء أو الاتصال مع النظام المعلوماتي المجرد، وعدم اشتراطها تحقيق غاية معينة، وهي بذلك تمنع إفلات المجرمين، كما أنها تشدد العقاب إذ ترتب على ذلك تعديل أو محو..الخ، أو الحصول على معلومات حكومية سرية كما جرمت فعل الاعتراض للبيانات. لما تقدم من مميزات للاتفاقية العربية نجد من المناسب الأخذ بنظر الاعتبار بنود هذة الاتفاقية لسن تشريع خاص بالجرائم المعلوماتية، خاصة وأن العراق قد صادق على هذة الاتفاقية[2]، كما نرى من الأفضل جعل صفة الموظف الذي يقوم بهذة الأفعال ظرفا مشدداً.

كما اصدرت منظمة التعاون الاقتصادي والتنمية تقريرا عام 1983 بعنوان الجرائم المرتبطة بالحاسوب وتحليل السياسة الجنائية والقانونية، إذ تناول تجريم الحد الأدنى لافعال سوء استخدام الحاسب، وألزمت الدول بضرورة تجريم هذه الأفعال في قوانينها، مثل الدخول غير المصرح به للنظام المعوماتي، وافشاء المعلومات للبيانات المخزونة داخل الحاسب، وأوصت اللجنة بضرورة أن تمتد الحماية، الى صور أخرى لاساءة استخدام الحاسوب، مثل الاختراق غير المأذون والتجارة بالأسرار، وفي عام 1992وضعت المنظمة توصيات إرشادية، للدول الأعضاء بتجريم التجسس المعلوماتي والذي يتضمن الاقتناء أو الاستعمال غير المشروع للمعطيات، وكذلك تجريم الدخول غير المشروع على البيانات أو نقلها، وأيضا اعتراض استخدام البيانات أو نقلها[3].

(1) د. هلالي عبد اللاه احمد، مرجع سابق، ص 61.

(2) وتجدر الاشارة الى أن المشرع العراقي قد صادق على الاتفاقية العربية في قانون تصديق الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المنشور في جريدة الوقائع العراقية رقم (31) لسنة 2013، العدد 4292، 30 أيلول 2013، ص 4.

(3) صغير يوسف، الجريمة المرتكبة عبر الانترنت، رسالة ماجستير، جامعة مولود معمدي كلية الحقوق والعلوم الساسية، الجزائر، 2013، ص 96 - 97.

ولم يقتصر التأكيد على حرمة الحياة الخاصة على المعاهدات والمنظمات الدولية، بل هنالك العديد من المؤتمرات، منها المؤتمر الدولي لحقوق الانسان في طهران لعام 1968 والذي أكد على (احترام السرية بالنسبة لأساليب التسجيل وحماية الحياة الخاصة.... واستخدام الالكترونيات التي قد تؤثر على حقوق الشخص والقيود التي يجب وضعها على هذا الاستخدام). ومؤتمر مونتريال الدولي لحقوق الانسان لعام 1968المنعقد في كندا، والذي أوصى بعدم قبول أدلة الاثبات المتحصلة من الوسائل التكنولجية، مثل أجهزة التسجيل على الأشرطة، وكذلك أجهزة التصنت على محادثات الافراد[1].

بعد استعراض الموقف الدولي من جريمة التجسس، نطرح سؤالا هل من مشروعية لهذة الجريمة على المستوى الدولي، حقيقة ظهر في ذلك أتجاهان أحدهما يرى بأن هنالك أساساً لمشرعية جريمة التجسس على المستوى الدولى، أما الاتجاه الآخر يرى عدم مشروعية التجسس على المستوى الدولي.

- **فبالنسبة للأتجاه الأول:**

يرى أن التجسس الدولي عملا مشروعا سواء كان في حالة السلم أم الحرب، وحجتهم هي أن التجسس يحقق للدولة حصننا ضد الأخطار الخارجية، كما يساعدها في وضع سياساتها العليا للدفاع الوطني على ضوء ماتحصل عليه من أسرار ومعلومات، مستندين في ذلك إلى الاتفاقات الدولية التي تبيح أعمال التجسس، ومنها معاهدة لاهاي لعام 1899 وبروتوكول جنيف لعام 1977، ومعاهدة لاهاي الملحقه لعام 1907 حيث حددت المادة (23) منها الأوامر والنواهي التي يحضر على المتحاربين استخدامها والتي لم تكن أعمال التجسس من بينها.

(1) أشارة اليها: د. كمال طلبة المتولي سلامة، دور الدولة في حماية السرية والاستثناءات الواردة عليها، ط 1، مركز الدراسات العربية، الجيزة، 2015، ص 36.

كما نصت المادة (24) على أن "خدع الحرب والقيام بالأعمال للحصول على المعلومات عن الطرف المعادي تعتبر أعمال مشروعة".

وكذلك المادة (31) منها حيث نصت على أن "الجاسوس الذي يعود وينضم إلى الجيش الذي ينتمي إليه ثم يقع في أسر العدو بعد ذلك يعامل أسير حرب ولا مسؤوليه عليه عن أعماله التجسسية السابقة" فهذا النص يسقط العقوبة عن الجاسوس الذي يتمكن من الهرب ولا مسؤولية عليه.

ويعرف التجسس المشروع بأنه: (البحث والتفتيش عن المستور من الأخبار، والمعلومات السرية الخاصة بالعدو، بواسطة أجهزة التجسس بقصد الاطلاع عليها والاستعانة بها في وضع الخطط في المواجهات)[1].

- **أما الاتجاه الثاني:**

والذي يرى عدم مشروعية التجسس، يذهب إلى أن الأفعال المحضورة المذكورة في معاهدة لاهاي والتي أستند عليها الاتجاه الأول واردة على سبيل المثال لا الحصر، كما أن فعل التجسس هو سلوك منبوذ دائما وأبدا، كما أن الجواسيس يهدفون إلى تحقيق الكسب المادي على حساب الحاق الضرر بأمن وسلامة الامم[2]. ومن وجهة نظري أؤيد الرأي الأخير وأن كان ذلك لا يتحقق على المستوى العملي، لأن الدول تسعى دائما الى أن تبقى هي الاقوى، من خلال التجسس على آخر ما تصل إليه الدول من تطور في مختلف المجالات العلمية أو العسكرية أو الاقتصادية...الخ، فالدول تجرم فعل هي أول القائمين به.

(1) سورية بنت محمد الشهري، المسؤولية الجنائية عن التجسس الالكتروني، رسالة ماجستير، جامعة نايف العربية للعلوم الامنية، الرياض، 2015، ص 22.

(2) للمزيد ينظر: د. محمود سليمان موسى، مرجع سابق، ص 182 وما بعدها.

الفرع الثاني

أساس تجريم التجسس المعلوماتي على الصعيد الوطني

تضمنت الدساتير المتعاقبة لجمهورية فرنسا التأكيد على حقوق الانسان، حيث تضمنت المقدمة لدستور 1791 الملغي نص إعلان حقوق الانسان المتعلق بمفهوم الحرية حيث نصت على "أنها حق الفرد في أن يفعل كل ما لايضر بالآخرين، ولا يمكن إخضاع ممارسات الحريات الطبيعية لقيود إلا من أجل تمكين أعضاء الجماعة من التمتع بحقوقهم، وهذة القيود لا يجوز فرضها إلا بالقانون"، كما أكد دستور 1958 النافذ على حقوق الإنسان حيث نصت مقدمته على أن "الشعب الفرنسي يعلم بصفة رسمية مدى تمسكه بحقوق الانسان"، وقد ذهب جانب من الفقه الفرنسي إلى أن الحرية الفردية تشمل حق الفرد في الاحتفاظ بأسراره الخاصة[1].

وقد جرم المشرع الفرنسي التجسس بصورة عامة في نص (الفقرة 6 من المادة 411) من قانون العقوبات الفرنسي الجديد لعام 1992 المعدل بالقانون رقم (913 - 93) الذي أصبح نافذ المفعول في عام 1994، والمتعلق بجرائم الخيانة والتجسس حيث نصت على أن " يعاقب بالاعتقال لمدة خمسة عشر سنة... كل من سلم إلى دولة أجنبية أو لمشروع أو منظمة أجنبية أو لأي جهة تخضع لسيطرة أجنبية أو لأحد عملائها، أو مهد في سبيل ذلك، معلومات، أساليب، أشياء، وثائق، معطيات مبرمجة آليا، أو فهارس، إذا كان في أستعمالها أو إفشائها أو تجميعها مايشكل بطبيعته ضررا بالمصالح الاساسية بالأمة"، من الملاحظ على النص المتقدم أنه تناول بالتجريم التجسس التقليدي والمعلوماتي، وذلك لأن محل

(1) د. محمد الشهاوي، الحماية الجنائية لحرمة الحياة الخاصة، دار النهضة العربية، القاهرة، 2005، ص 361.

الجريمة في النص المتقدم هو قد يكون وثائق أو معطيات مبرمجة آليا، وهو مايدل على تجريم التجسس سواء كان وثائق ورقية أو بيانات معالجة آليا، وفيما يخص الحياة الخاصة.

فقد جرمت (الفقرة 1 من المادة 226) من قانون العقوبات الفرنسي أيضا، فعل الالتقاط أو التنصت أو التسجيل أو النقل للحديث الخاص أو الصورة الشخصية، حيث نصت على أن "يعاقب...كل من يعتدي أراديا أو عمدا على حرمة الحياة الخاصة للغير بأي وسيلة كانت: 1 - بالتنصت أو بتسجيل أو بنقل الأحاديث التي تصدر عن شخص بصفه سرية أو خاصة دون رضاه. 2 - بالتقاط أو تسجيل أو بنقل صورة شخص يوجد في مكان خاص دون رضاه"، من الملاحظ على النص استخدامه عبارة إراديا أو عمدا وهو أن الفعل في الحالة الأولى قد يكون تحت إكراه مادي أو معنوي، ومن الجدير بالذكر هو أن المشرع الفرنسي قد حدد شروط التنصت على المكالمات الهاتفية في القانون الصادر في 10 تموز عام 1991، والذي كان قبل ذلك محل اجتهاد للفقه، ومن هذة الشروط هو عدم التنصت على المكالمات الهاتفية الا بقرار مسبب من قاضي التحقيق وتحت إشرافه ومراقبته، وكذلك لا يمكن التنصت على المخابرات السلكية واللاسلكية الا في حالات الضرورة القصوى[1].

كماجرمت (الفقرة 22 من المادة 226)، إفشاء البيانات الإسمية بما يضر صاحب الشأن، حيث نصت على أن "يعاقب... كل شخص كان قد أستقبل أو تلقى بمناسبة التسجيل أو التنصت أو النقل، أو أي إجراء آخر من اجراءات المعالجة الالكترونية بيانات أسمية من شأن أفشائها الاضرار بأعتبار صاحب الشأن، أو حرمة حياته الخاصة، وقام بنقلها الى من لا حق له بالعلم بها، وإذا وقع

(1) أشارة اليها: نزيه نعيم شلال، دعاوى التنصت على الغير، ط 1، منشورات زين الحقوقية، بيروت، 2010، ص 59.

هذا الإفشاء[1] للبيانات الإسمية بطريق الاهمال تكون العقوبات...ولا تقام الدعوى العمومية وفقا للفقرتين السابق الاشارة إليهما، إلا من خلال شكوى المجني...".

أما عن التنصت على المراسلات في إطار التجارة الالكترونية، فقد جرمت (الفقرة 9 من المادة 432) من قانون العقوبات الفرنسي الجديد، التقاط أو فض المراسلات أو كشف محتواها حيث نصت على أن " 1 - كل شخص عام أو مكلف بخدمة عامة يعاقب... إذا قام عند مباشرته لعمله أو بمناسبته بالأمر أو التسهيل أو القيام، في غير الحالات المقررة قانونا باختلاس أو إلغاء أو فض المراسلات أو كشف محتوها.2 - كل شخص عام أو مكلف بخدمة عامة أو بأعمال استغلال خدمة الاتصالات، أو بأعمال تقديم خدمة الاتصالات، بالحبس... إذا قام عند مباشرته لعمله بالأمر أو التسهيل أو القيام، في غير الحالات المقررة قانونا بالتقاط أو اختلاس مراسلات تتم أو تنقل أو تصل بطريق الاتصالات، وكذلك باستعمال أو فض محتواها ". يلاحظ على الفقرتين المتقدمتين أنهما قد عالجا جريمتين متميزتين، فالفقرة الاولى عالجت حالة الاعتداء على المراسلات بالمعنى الضيق وذلك لأنها استخدمت كلمة "فض"، أما الفقرة الثانية فهي تناولت تجريم الاعتداء على المراسلات التي تتم عبر خدمة الاتصالات، والتي قد تكون سمعية كالتلفون أو بصرية كالانترنت أو مكتوبة كالفكس والتلكس، وهو ما يشير إلى عدم اقتصارها على المراسلات التلفونية التي تتم خلال شبكة الانترنت[2]، وأرى أن نص المادة (432) جرم التنصت على المراسلات الخاصة بالتجارة الالكترونية مستخدما فعل الالتقاط أو الاختلاس، كما أنها توسعت في معنى التنصت ليشمل الاتصالات

(1) الافشاء يقصد به: (أطلاع الغير على السر بأي طريقة كانت مشافهة أو كتابة). ينظر: د. حسني عبد السميع أبراهيم، الجرائم المستحدثة عن طريق الانترنت (دراسة مقارنة بين الشريعة والقانون)، دار النهضة العربية، القاهرة، 2011، ص 592.

(2) للمزيد: عبد الفتاح بيومي حجازي، التجارة الالكترونية وحمايتها القانونية، دار الفكر الجامعي، الاسكندرية، 2004، ص 399 وما بعدها. شول بن شهرة و ماجد مدوخ، ورقة علمية مقدمة الى الملتقى الدولي الاقتصادي الإسلامي، الواقع ورهانات المستقبل، بعنوان (حماية الخصوصية في المعاملات المالية الاسلامية / بيانات عملاء العمليات المصرفية الالكترونية نموذجا(، ص 14.

السمعية والبصرية والمكتوبة، وهو أمر في تقديرنا لا يتماشى مع جريمة التنصت، حيث أن الركن المادي في جريمة التنصت، يشترط به أن يكون المتنصت قادر على السمع، وأن يكون الصوت مسموعا، وأن يكون الصوت مرسل عن طريق شبكة الانترنت، أو إحدى أجهزة الكومبيوتر، ويحصل التنصت دون سبب قانوني[1].. الخ، وهو أمر غير متصور الحصول على ماهو بصري أو مكتوب، وكان من الأفضل استخدام لفظ التنصت أو الالتقاط أو الدخول غير المشروع على الاتصالات أو المراسلات الالكترونية.

أما في التشريع الامريكي فعلى الرغم من تأكيد الدساتير على تقديس حقوق الإفراد، إلا أنها جاءت خالية من نص يأكد حرمة الحياة الخاصة[2]، إلا أن الاتفاقية الأمريكية لحقوق الانسان لعام 1969 تضمنت التأكيد على حرمة الحياة الخاصة والمراسلات للأفراد في (الفقرة 2 من المادة 11) منها حيث نصت على"لا يجوز أن يتعرض أحد لتدخل أعتباطي أو تعسفي في حياته الخاصة أو في شؤون أسرته أو منزله أو مراسلاته، ولا أن يتعرض لأعتداء غير مشروع على شرفه أو سمعته".

أما عن القانون الفدرالي الاتحادي رقم (18) لسنة 1984 المعدل[3] الخاص بأساءة استخدام الحاسب، فقد جرم التجسس المعلوماتي والذي يتم باختراق حواسيب الولايات المتحدة الحكومية أو المالية أو مؤسسة اقتصادية أو الاتصالات التي تتم داخل الولايات المتحدة أو خارجها[4].

(1) د. خالد ممدوح أبراهيم، فن التحقيق...، مرجع سابق، ص 341.

(2) د. محمد الشهاوى، مرجع سابق، ص 364.

(3) من الجدير بالذكر: هو أن التشريع الفدرالي الامريكي الخاص بجرائم الحاسب الآلي تم تعديل عدة مرات وفي كل مرة يدخل التعديل تحت أطار أو تسمية مختلفة، ففي عام 1984 تحت تسمية قانون تزيف آليات الدخول والاساءة والاحتيال عبر الكومبيوتر، وفي عام 1994 فقد تم تعديلة ضمن تشريع قانون التحكم في العنف الاجرامي وتنفيذ القانون، وفي عام 1996 صدر بمقتضى قانون البنية القومية للمعلومات. ينظر: د. خالد ممدوح أبراهيم، الجرائم المعلوماتية، مرجع سابق، ص 264 وما بعدها.

(4) د. حسام محمد نبيل الشنراقي، الجرائم المعلوماتية دراسة تطبيقية مقارنة على جرائم الاعتداء على =

إذ نصت (**الفقرة أ من المادة** 1030) **على** تجريم الدخول غير المشروع للحواسيب الحكومية أو المتعلقة بأعمال الحكومة " 1 - الدخول العمدي إلى جهاز الحاسوب بدون تصريح أو تجاوز للتصريح الممنوح له، ويحصل بأية وسيلة على معلومات تقررت من قبل حكومة الولايات المتحدة بناء على أمر تنفيذي وتصريح برلماني يتطلب الحماية، ضد الافشاء غير المخول به لأسباب تتعلق بالدفاع الوطني أو العلاقات الأجنبية. 2 - الوصول عمدا إلى الحاسوب بدون ترخيص، أو تجاوز الترخيص الممنوح بقصد الحصول على معلومات واردة في سجل مالي بمؤسسة مالية، أو أن تشمل هذه المعلومات المتضمنة في ملف وكالة أو معلومات من أي حاسب محمي إذا تعلق بمحتوى اتصالات خارجية أو بين الولايات. 3 - الوصول العمدي بدون ترخيص لأي حاسوب غير عام يخص إحدى إدارات أو وكالات الولايات المتحدة مخصص لاستعمال حكومة الولايات المتحدة، أو لم يكن مخصص لها ولكن استعمل من قبل أو لأجل حكومة الولايات المتحدة الأمريكية وكان ذلك التصرف مؤثرا على ذلك الاستعمال من قبل أو لأجل حكومة الولايات المتحدة"، من الملاحظ على النص أنه غامض وغير واضح وأنه يساعد المجرمين للإفلات من العقاب في حال استخدامهم حاسب وشبكات من خارج الولايات المتحدة والدخول الى أنظمة الحاسب في الولايات المتحدة أو استخدامها للإعتداء على أنظمة تقع خارجها[1]، كما أنه اشترط بالفقرة الثانية أن يكون الحاسب محمي، فهذا يعني لا تقوم الجريمة إذا كان الحاسب غير محمي، كما اشترط توافر القصد الجرمي في الفقرة الثانية بخلاف الفقرة الأولى والثالثة التي تعاقب على الدخول المجرد، وأرى من وجهة نظري أشتراط القصد الجرمي الخاص، أمر غير سليم لأن الحماية تشمل الحواسيب الحكومية من أي اعتداء بصرف النظر عن القصد الجرمي،

= التوقيع الالكتروني، دار الكتب القانونية، مصر، 2013، ص 144.

(1) جرائم الانترنت. متاح على موقع ستار تايمز. وقت وتاريخ الزيارة: 100، 2015/8/15.

خاصة وأن القصد الجرمي مسألة نفسية تقودنا للبحث عن قرائن ودلالات من أجل إثباته هذا من جهة، ومن جهة أخرى يساعد المجرمين على الافلات من العقاب بحجة عدم علمهم وأن دخولهم كان بمحض الصدفة، يضاف إلى ماتقدم أن الجرائم المعلوماتية تتميز بصعوبة الاثبات. ويجد المتتبع لموقف المشرع الأمريكي أنه على الرغم من أن قانون مكافحة إساءة استخدام الحاسب قد جرم التجسس المعلوماتي، إلا أن القانون الصادر من الكونغرس لعام 1968 كان قد منح رئيس الولايات المتحدة الحق بإصدار الامر بالتنصت واستراق السمع على المكالمات الهاتفية، لحماية الأمن الداخلي من أعمال التجسس الخارجي[1]، وأرى أن في ذلك تهديداً لسرية أي شخص طبيعي أو معنوي، إذ يستطيع الرئيس الامريكي انتهاك سرية البيانات أو المعلومات الخاصة متى ما ادعى أن هنالك تهديداً لأمن الولايات المتحدة.

أما بالنسبة للتشريعات العربية فقد تضمن دستور الامارات العربية المتحدة لعام 1971، التأكيد على حرية المراسلات في المادة (31) منه إذ نصت على " حرية المراسلات البريدية والبرقية وغيرها من وسائل الاتصال وسريتها مكفولتان وفقا للقانون"، كما جَرّم قانون العقوبات الاماراتي رقم (3) لعام 1987 الاعتداء على الحياة الخاصة حيث نصت المادة (380) على أن "يعاقب... من فض رسالة أو برقية بغير رضاء من أرسلت إليه أو استرق السمع على مكالمة هاتفية. ويعاقب... إذا أفشى سر الرسالة أو البرقية أو المكالمة لغير من وجهت إليه من دون إذن متى كان من شأن ذلك إلحاق الضرر بالغير".

أما في أطار المرسوم بالقانون رقم (5) لعام 2012 لمكافحة جرائم تقنية المعلومات الذي ألغى القانون السابق رقم (2) لعام 2006.

(1) أشارة اليه: نزيه نعيم شلال، مرجع سابق، ص 60.

فقد جاء بنصوص أكثر شمولا حيث نصت المادة (2) على أن "1 - يعاقب...كل من دخل موقعا الكترونيا أو نظام معلومات الكتروني أو شبكة معلوماتية، أو وسيلة تقنية معلومات، بدون تصريح أو بتجاوز حدود التصريح، بالبقاء فيه بصورة غير مشروعة.2 - تكون العقوبة...إذا ترتب على أي فعل من الافعال المنصوص عليها بالفقرة (1) من هذة المادة الغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغير أو نسخ أو نشر أو إعادة نشر أي بيانات أو معلومات.3 - تكون العقوبة... إذا كانت البيانات أو المعلومات محل الأفعال الواردة في الفقرة (2) من هذة المادة شخصية".

كما تناولت المادة (21) تجريم الاعتداء على الحياة الخاصة حيث نصت على أن "يعاقب.كل من استخدم شبكة معلوماتية، أو نظام معلوماتي ألكتروني، أو إحدى وسائل تقنية المعلومات، في الاعتداء على خصوصية شخص في غير الأحوال المصرح بها قانونا بإحدى الطرق التالية: 1 - استراق السمع أو اعتراض أو تسجيل أو نقل أو بث أو افشاء محادثات أو اتصالات ومواد صوتية أو مرئية. 2 - إلتقاط صور الغير أو إعداد صور ألكترونية أو نقلها أو كشفها أو نسخها أو الاحتفاظ بها. 3 - نشر أخبار أو صور ألكترونية أو صور فوتوغرافية أو مشاهد أو تعليقات أو بيانات أو معلومات ولو كانت صحيحة وحقيقية. كما يعاقب...كل من استخدم نظام معلوماتي الكتروني، أو أحدى وسائل تقنية المعلومات، لإجراء أي تعديل أو معالجة على تسجيل أو صورة أو مشهد، بقصد التشهير أو الاساءة إلى شخص آخر، أو الاعتداء على خصوصيته أو انتهاكها". وأرى أن النص المتقدم هو نص جيد، ومن الأفضل وضعه بعين الاعتبار عند تجريم الاعتداء على الخصوصية بواسطة الوسائل التقنية في التشريع العراقي، إذ لم أجد له مثيلاً في القوانين محل المقارنة.

وتجرم المادة (4) التجسس على البيانات الحكومية وذلك بأفشائها أو نشرها أو إعادة نشرها حيث نصت على أن "يعاقب...كل من دخل بدون تصريح إلى موقع ألكتروني، أو نظام معلوماتي ألكتروني، أو شبكة معلوماتية، أو وسيلة تقنية معلومات، سواء كان الدخول بقصد الحصول على بيانات حكومية، أو معلومات سرية [1]خاصة بمنشأة مالية أو تجارية أو اقتصادية. وتكون العقوبة... إذا تعرضت هذة البيانات أو المعلومات للإلغاء أو الحذف أو الاتلاف أو التدمير أو الافشاء أو التغيير أو النسخ أو النشر أو اعادة النشر"، ما يلا حظ على النص أنه قد أشترط أن تكون المعلومات الاقتصادية أو التجارية أو الاقتصادية سرية، بعكس البيانات الحكومية فإنه لم يشترط السرية وهو موقف جيد على اعتبار أن الصفة الغالبة عليها سرية ولا يجوز الاعتداء عليها.

وتجرم المادة (12) التجسس على أرقام أو بيانات بطاقات الائتمان أو الحسابات المصرفية بانتهاك سريتها حيث نصت على أن "يعاقب...كل من توصل بغير حق، عن طريق استخدام الشبكة المعلوماتية أو نظام معلوماتي ألكتروني أو إحدى وسائل تقنية المعلومات، إلى أرقام أو بيانات بطاقة إئتمانية أو الكترونية أو أرقام أو بيانات حسابات مصرفية، أو أي وسيلة من وسائل الدفع الالكتروني. وتكون العقوبة...إذا قصد من ذلك استخدام البيانات والأرقام في الحصول على أموال الغير، أو الاستفادة بما تتيحه من خدمة...ويعاقب بذات العقوبة المنصوص عليها بالفقرة السابقة كل من نشر أو إعادة نشر أرقام أو بيانات بطاقات ائتمانية أو الكترونية أو أرقام أو بيانات حسابات مصرفية تعود للغير، أو أي وسيلة أخرى من وسائل الدفع الالكتروني". يلاحظ على النص أنه شامل في تجريم أي إعتداء على البيانات أو الأرقام للحسابات المصرفية أوبطاقات الإئتمان أو أي من وسائل الدفع الالكتروني حيث جاء النص بالإضافة للشمولية فإنه جاء مَرِناً أيضا، وذلك

(1) يقصد بالسرية " أي معلومات أو بيانات غير مصرح للغير الاطلاع عليها أو بأفشاءها الا بأذن مسبق ممن يملك هذا الاذن " المادة (1) من مرسوم مكافحة الجرائم المعلوماتية الاماراتي.

بترك الباب مفتوحاً لوسائل ارتكاب الجريمة باستخدامه عبارة "أو أحدى وسائل تقنية المعلومات" أضافة الى أن محل الجريمة جاء مرنا بعبارة " أي من وسائل الدفع الالكتروني"، وهو أمر جيد.

كما جرمت المادة (15) صور أخرى من التجسس المعلوماتي وهي أعتراض أو إلتقاط الاتصالات التي تتم عن طريق الشبكات حيث نصت على أن "يعاقب كل من إلتقط أو اعترض عمداً وبدون تصريح أي أتصال عن طريق أي شبكة معلوماتية. فإذا أفشى أي شخص المعلومات التي حصل عليها عن طريق استلام أو اعتراض الاتصالات بغير وجه حق، فإنه يعاقب بالحبس مدة لا تقل عن سنة واحدة"، يلاحظ على النص أنه يعاقب على فعل الالتقاط أو الاعتراض للأتصالات، ويشدد العقاب على إفشاء هذا الاتصال ممن اعترضها أو استلمها، و يأخذ على النص أنه حدد الاتصالات التي تتم بواسطة الشبكات المعلوماتية، وبهذا يخرج من التجريم اعتراض أو استلام الاتصالات التي تتم عن طريق الهواتف بأستخدام شبكات الاتصالات.

تجرم المادة (22) كشف[1] الموظف للمعلومات التي تصل إليه بمناسبه وظيفته أو بسببها حيث نصت على أن "يعاقب...كل من استخدم بدون تصريح، أي شبكة معلوماتية، أو موقعا الكترونيا، أو وسيلة تقنية معلومات، لكشف معلومات سرية حصل عليها بمناسبة عمله أو بسببه".

وبالنسبة للتشريع السعودي فقد تناول حماية الحياة الخاصة بدستورها الصادر عام 1992 حيث منعت المادة (40) منه، الاطلاع أو الاستماع للمراسلات البرقية والبريدية والمخابرات الهاتفية حيث نصت على أن " المراسلات البرقية والبريدية والمخابرات الهاتفية وغيرها من وسائل الاتصالات مصونة، ولايجوز مصادرتها أو تأخيرها أو الاطلاع عليها أو الاستماع إليها إلا في الحالات التي يبينها

(1) الكشف يعني لغة: رفعك الشئ عما يغطيه. ينظر: الصاحب بن عباد، المحيط في اللغة، ج2، مطبعة المعارف، بغداد، 1975، ص 26.

النظام ". ويجرم المنظم السعودي إفشاء أسرار الدفاع بصورته التقليدية بعدة أنظمة منها، نظام العقوبات العسكري السعودي رقم 95/8/10 لعام 1366، حيث جرم التشريع السعودي الخيانة العظمى والتي تشمل افعال التجسس لصالح العدو بما يضر المصالح العسكرية أو السياسية للملكة العربية السعودية[1].

وذلك في (الفقرة ج من المادة 24) حيث نص على أن "الخيانة الحربية ومن ضمنها التجسس والسعي في الاطلاع على أسرار الدولة لمصلحة العدو، بتدبير المكائد والمؤامرات السرية لقلب نظام الحكم، والتدمير للمؤسسات والمنشآت الحربية وقطع حبل المواصلات والمخابر والحيلولة دون تأمينها واستعمالها خلسه في مصلحة العدو....". وكذلك نظام عقوبات نشر الوثائق والمعلومات السرية وأفشائها السعودي رقم (35) لعام 1432، حيث جرمت المادة (1) منه، إفشاء الموظف للأسرار التي يطلع عليها بحكم عمله، والتي يؤدي افشاؤها الى الاضرار بالامن الوطني ومصالح وسياسات وحقوق الدولة السعودية. و يجرم نظام محاكم الوزراء بالمادة (2) التجسس التقليدي واعتبارها من جرائم الخيانه العظمى[2]، حيث عاقب من يفشي سرا من أسرار الدفاع ويسلمها الى دولة أجنبية من الوزراء أو من في حكمهم بالسجن خمسة وعشرين سنة. وجرمت المادة (5) منه أيضا على معاقبة من يفشي قرارات ومداولات مجلس الوزراء. أما نظام المنافسة السعودي الصادر بالمرسوم رقم (25) لعام 1425، فقد جرم بالمادة (13) إفشاء الموظفين وأعضاء مجلس المنافسة للمعلومات السرية أو السجلات التي حصل عليها أثناء جمع الاستدلالات أو التحقيقات[3]، حيث نصت على " يعاقب كل من أفشى سرا له

---

(1) منصور بن ناصر العضيلة، جريمة الخيانة العظمى في النظام العسكري السعودي وعقوبتها(دراسة مقارنة)، رسالة ماجستير، جامعة نايف العربية للعلوم الامنية، 2013، ص 44 - 45.

(2) وليد بن سعد محمد عوشن، الحماية الجنائية لأسرار الدولة في النظام السعودي، رسالة ماجستير، جامعة نايف العربية للعلوم الامنية، 2013، ص 136 - 137.

(3) وليد بن سعد محمد عوشن، مرجع نفسه، ص 137.

علاقة بعمله طبقا لأحكام (الفقرة 5 من المادة 11) من هذا النظام، أو حقق نفعاً بطريقة مباشرة أو غير مباشرة، بغرامة مالية...".

أما عن النظام السعودي لمكافحة الجرائم المعلوماتية رقم (17) لعام 2007 والذي تناول التجسس المعلوماتي بالتجريم، حيث جرمت المادة (3) أفعال التنصت أو الالتقاط أو الاعتراض إذ نصت على أن " 1 - التنصت على ماهو مرسل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي - دون مسوغ نظامي صحيح - أو إلتقاطة أو اعتراضه. 4 - المساس بالحياة الخاصة عن طريق إساءة استخدام الهواتف النقالة المزودة بالكاميرا، أو ما في حكمها"، ما يلاحظ على النص بفقرته الاولى أنه حصر وسيلة ارتكاب التجسس المعلوماتي بالشبكة المعلوماتية أو إحدى أجهزة الحاسب الآلي[1]، حيث أرى أنه أمر غير دقيق وذلك لأن فعل التنصت أو الالتقاط ممكن أن ترتكب بواسطة الهواتف، لذا كان من الأفضل أستخدام عبارة أو أي وسيلة تقنية أخرى وبذلك تدخل الهواتف ضمن نطاق التجريم، إضافة إلى ذلك تنتفي الحاجة إلى الفقرة الرابعة لأنها لم تأتِ بجديد حيث أن فعل الالتقاط يشمل التصوير بأي وسيلة كانت سواء آلة كاميرا أو هواتف تحوي كاميرا. وتعد الافعال المتقدمة من صور التجسس المعلوماتي لأن الغاية منها هو الوصول إلى أسرار الآخرين دون رضاهم سواء قصد الجاني الاضرار بالاخرين أم لم يقصد، وذلك لأن النموذج القانوني للجريمة يكتمل بمجرد الاطلاع الغير مصرح به[2].

أضافة الى ماجاء (بالفقرة 4 من المادة 3) فقد أفرد المشرع السعودي وفي إطار الحياة الخاصة أيضا نص المادة (5) على أن " يعاقب... كل شخص يرتكب أيا من الجرائم المعلوماتية الاتية: 1 - الدخول غير المشروع لإلغاء بيانات خاصة، حذفها، أو تدميرها، أو تسريبها، أو إتلافها، أو تغييرها، أو إعادة نشرها ".

(1) سورية بنت محمد الشهري، مرجع سابق، ص 41.

(2) سورية بنت محمد الشهري، مرجع نفسه، ص 24.

وجرمت المادة (7) **التجسس على البيانات الحكومية المتعلقة بالامن أو الاقتصاد الوطني حيث نصت على أن** " يعاقب...كل شخص يرتكب أيا من الجرائم المعلوماتية الاتية: 2 - الدخول غير المشروع الى موقع الكتروني، أو نظام معلوماتي مباشرة، أو عن طريق الشبكة المعلوماتية، أو إحدى أجهزة الحاسب الآلي، للحصول على بيانات تمس الأمن الداخلي، أو الخارجي للدولة أو اقتصادها الوطني" نجد في النص المتقدم أنه قد جرم الاعتداء على أمن الدولة الخارجي والتي من بينها جريمة التجسس، التي تمثل اعتداء على الأمن الخارجي للدولة السعودية، وتناول بالحماية الاقتصاد الوطني من أفعال التجسس، وما يأخذ على النص اشتراطه القصد الجرمي الخاص.

أما عن التشريع العراقي، فقد منعت المادة (40) **من دستور جمهورية العراق لعام** 2005 **التجسس المعلوماتي على الاتصالات والمراسلات الماسة بالحياة الخاصة حيث نصت على أن** "حرية الاتصالات والمراسلات البريدية والبرقية والهاتفية والالكترونية وغيرها مكفولة، ولا يجوز مراقبتها أو التنصت عليها، أو الكشف عنها، إلا لضرورة قانونية وأمنية وبقرار قضائي"، ما يلاحظ على النص أنه منع الاعتداء على المراسلات البريدية والبرقية والهواتف دون ذكر النظم المعلوماتية أو الشبكات المعلوماتية..الخ، كما منع الاعتداء على الاتصالات وغيرها، لضرورة قانونية وأمنية، والادق أستخدام عبارة لضرورة قانونية أو أمنية للتخيير بينهما، ونقترح تعديل النص على النحو الاتي "لا يجوز الاعتداء على الانظمة المعلوماتية أو الشبكات المعلوماتية أو المواقع الالكترونية أو المراسلات البريدية أو البرقية أو الهاتفية أو غيرها من وسائل التقنية، بالتنصت أو المراقبة أو الكشف أو الافشاء أو الاعتراض أو الالتقاط أو الدخول غير المشروع أو غير ذلك، الا لضرورة قانونية أو أمنية وبقرار قضائي".

وفي إطار قانون العقوبات العراقي فقد جرم أفعال التجسس التقليدية، حيث عاقبت المادة (328) الموظف أو المكلف بخدمة عامة الذي يعتدي على حرمة الحياة الخاصة إذ نصت على أن " يعاقب بالسجن مدة لا تزيد على سبع سنوات أو بالحبس كل موظف أو مستخدم في دوائر البريد والبرق والتلفون وكل موظف أو مكلف بخدمة عامة فتح أو اتلف أو أخفى رسالة أو برقية أودعت أو سلمت للدائرة المذكورة أو سهل لغيره ذلك أو أفشى سرا تضمنته الرسالة أو البرقية ". وأرى أن في حال عدم إقرار مشروع قانون الجرائم المعلوماتية نقترح تعديل نصوص قانون العقوبات العراقي.

فبالنسبة للمادة (328) من قانون العقوبات العراقي يكون النص المقترح " يعاقب بالسجن مدة لا تزيد على سبع سنوات أو بالحبس كل من اعتدى على الانظمة المعلوماتية أو الشبكات أو المواقع الالكترونية أو البريد أو البرق أو التلفون أو غيرها من الوسائل التقنية، أو قام بفتح أو إفشاء أو نسخ أو نشر أو إتلاف أو إخفاء لبيانات أو معلومات أو صور أو غير ذلك. إذا أرتكبت تلك الافعال من موظف أو مكلف بخدمة عامة عد ذلك ظرفا مشددا".

وفي إطار الحياة الخاصة أيضا نجد أن المادة (438) جَرَّمَتْ أفعال النشر للصور أو للاخبار أو للتعليقات التي تمس الحياة الخاصة، حتى وإن كانت صحيحة إذا كان من شأن ذلك الاساءة لصاحب الشأن بالقول " يعاقب بالحبس مدة لاتزيد على سنة وبغرامة لاتزيد على مائة دينار أو بأحدى هاتين العقوبتين. 1 - من نشر بأحدى طرق العلانية أخبارا أو صورا أو تعليقات تتصل بأسرار الحياة الخاصة أو العائلية للأفراد ولو كانت صحيحة أذا كان من شأن نشرها الاساءة اليهم. 2 - من أطلع من غير الذين ذكروا في المادة (328) على رسالة أو برقية أو مكالمة تلفونية فأفشاها لغير من وُجّهَتّ إليه أذا كان من شأن ذلك إلحاق ضرر بأحد ". من الملاحظ على النصيين إنهما جرما الاعتداء على الحياة الخاصة

سواء صدر الاعتداء من موظف أو شخص عادي، إلا أنهما ضيقا من نطاق الحماية للحياة الخاصة، حيث أستبعدا من الحماية جانب كبير من عناصر الحياة الخاصة، كالحديث الخاص والتسجيل والتنصت والنقل للحديث..الخ[1].

لذلك نقترح تعديل نص المادة (438) أيضاعلى النحو الاتي "يعاقب بالحبس مدة لاتزيد على ثلاثة سنوات وبغرامة لاتزيد على عشرة ملايين أو بأحدى هاتين العقوبتين، كل من نشر أو نقل أو كشف أو نسخ أو سجل أو بث أو أفشى أو احتفظ أو التقط أو أعترض أو تنصت أو غير ذلك، لأخبارٍ أو صورٍ للغير أو مشاهد أو تعليقات أو محادثات أو أتصالات ومواد صوتية أو مرئية أو بيانات أو معلومات ولو كانت صحيحة وحقيقية، أو إعداد صور الكترونية أو فوتوغرافية تتصل بحرمة الحياة الخاصة أو العائلية للأفراد، سواء باستخدم نظام معلوماتي ألكتروني أو شبكة معلوماتية، أو إحدى وسائل تقنية المعلومات، أو غير ذلك".

كما نصت المادة (363) من قانون العقوبات العراقي على أن "يعاقب بالحبس من تسبب عمدا في ازعاج غيره باساءة استعمال اجهزة الاتصال السلكية او اللاسلكية"، يمكن الاستعانة بهذا النص في محاسبة مرتكبي جرائم الاعتداء على حرمة الحياة الخاصة بشكل مؤقت[2] لحين إقرار مشروع الجرائم المعلوماتية العراقي، كما نقترح تعديله على النحو الاتي "يعاقب بالحبس من تسبب عمدا في ازعاج أو انتهاك سرية البيانات أو المعلومات أو النظام المعلوماتي أو الموقع الالكتروني أو شبكة المعلومات أو غيرها من وسائل التقنية التابعة للغير".

---

(1) د. طارق صديق رشيدكه ردى، حماية الحرية الشخصية في القانون الجنائي (دراسة تحليلية مقارنة)، ط1، منشورات الحلبي الحقوقية، بيروت، 2011، ص 218.

(2) سمير ابراهيم جميل قاسم العزاوي، المسؤولية الجنائية الناشئة عن إساءة استخدام الانترنت، أطروحة دكتورا، جامعة بغداد – كلية القانون، 2005، ص 92.

وفي إطار جريمة التجسس الماس بأمن الدولة فقد جرمت المادة (158) السعي[1] لدى دولة أجنبية أو التخابر[2] معها أو ممن يعمل لمصلحتها، للقيام بأعمال عدائية ضد العراق قد ينتج عنها حرباً أو قطعاً للعلاقات الدبلوماسية.

حيث نصت على أن "يعاقب بالاعدام أو السجن المؤبد كل من سعى لدى دولة أجنبية أو تخابر معها أو مع أحد ممن يعملون لمصلحتها للقيام بأعمال عدائية ضد العراق.... ".

كما جرمت المادة (159) التخابر أو السعي لدى دولة أجنبية معادية[3]، **حيث نصت على** "يعاقب بالاعدام كل من سعى لدى دولة أجنبية معادية أو تخابر معها أو مع أحد ممن بعملون لمصلحتها لمعاونتها في عملياتها الحربية ضد العراق..." وتختلف هذة المادة عن التجريم المنصوص عليه في المادة (164) والتي تجرم السعي أو التخابر مع دولة ليست في حالة حرب مع العراق[4]، حيث نصت على أن "يعاقب بالاعدام: 1 - من سعى لدى دولة أجنبية أو لدى أحد ممن يعملون لمصلحتها أو تخابر مع أي منهما، وكان من شأن ذلك الاضرار بمركز العراق الحربي أو السياسي أو الاقتصادي. 2 - من أتلف عمدا أو أخفى أو سرق أو زور أوراقا أو وثائق وهو يعلم أنها تصلح لإثبات حقوق العراق قبل دولة أجنبية أو تتعلق بأمن الدولة الخارجي أو بأي مصلحة وطنية أخرى". ما يلاحظ على الفقرة الأولى

(1) يقصد بالسعي: كل فعل او نشاط يصدر من الجاني يقصد به تقديم خدمه لدولة اجنبية للقيام بعمل عدائي سواء تحقق العمل ام لم يتحقق. ينظر: د سعد أبراهيم الاعظمي، جرائم التجسس في التشريع العراقي (دراسة مقارنة)، رسالة ماجستير، كلية القانون جامعة بغداد، 1981، ص 94.

(2) يقصد بالتخابر: هو كل اتصال بغض النظر عن الوسيلة أو الطريقة التي يتم بها لمرة او لعدة مرات اتصالا غير مشروع بدولة اجنبية. للمزيد ينظر: علي حامد عياد، مرجع سابق، ص 168.

(3) يقصد بدولة معادية: هي الدولة التي تكون في حالة حرب مع العراق. ينظر: د. سعد أبراهيم الاعظمي، جرائم التجسس...، مرجع سابق، ص 129.

(4) د. سعد أبراهيم الاعظمي، جرائم التجسس...، مرجع سابق، ص 129.

من المادة أنها تجرم الفعل حتى لو كان الضرر محتمل وهو مايتفق مع طبيعة جريمة التجسس باعتبارها من جرائم الخطر كما سنبين ذلك بالمبحث الثاني.

وجرمت المادة (162) فعل نقل[1] الأخبار المتعلقة بالدفاع للعدو، كما جرمت المادة (177) افشاء أو إتلاف أو تسليم أسرار الدفاع أو الوثائق أو الاسرار التي تعتبر من اسرار الدفاع، حيث نصت على أن " يعاقب بالسجن المؤبد: 1 - كل من حصل بأية وسيلة على شئ يعتبر من أسرار الدفاع عن البلاد بقصد إتلافه لمصلحة دولة أجنبية أو أفشائه لها أو لأحد ممن يعملون لمصلحتها. 2 - كل من سلم أو أفشى سرا من أسرار الدفاع عن البلاد إلى دولة أجنبية أو إلى أحد ممن يعملون لمصلحتها. 3 - كل من أتلف.... وتكون العقوبة الاعدام إذا كان الجاني شخصا مكلف بخدمة عامة أو إذا ارتكبت الجريمة في زمن الحرب أو كانت الدولة الاجنبية معادية". كما جرمت المادة (178) فعل الإذاعة أو الأفشاء حيث نصت على أن "يعاقب بالسجن مدة لاتزيد على عشرة سنين: 2 - من أذاع أو أفشى بأية وسيلة سرا من أسرار الدفاع. 3 - من نظم أو استعمل أية وسيلة من وسائل الاتصال بقصد الحصول على سر من أسرار الدفاع عن البلاد أو بقصد تسليمه أو إذاعته".

نخلص من النصوص المتقدمة أنها لم تشترط وسيلة معينة، وبالتالي يمكن أن يتم التجسس بأي طريقة للحصول على أسرار الدفاع مثلا باستخدام تقنية المعلومات لإجراء تنصت أو أعتراض أو التقاط أو دخول غير مشروع إلى معلومات أو بيانات تعد من أسرار الدفاع، أيا كان مكان وجودها سواء كانت في حاسب أو

(1) النقل يعني باللغة: نقل الحديث أذ يقال، ناقلت فلان الحديث أذ حدثته وحدثك. ويعني أيضا، هو تحويل الشئ من موضع الى موضع أخر. ينظر: الصاحب بن عباد، مرجع سابق، ج1، ص 479. إسماعيل بن حماد الجوهري، تحقيق أحمد عبد الغفور عطار، الصحاح في اللغة، ج 1، ط 4، دار العلم للملايين، بيروت، 1990، ص 229.

موقع الكتروني..الخ، يضاف إلى ذلك أن المشرع كان موفقا في إيراده عبارة "يعتبر من أسرار الدفاع" ليشمل أي معلومات أو بيانات تتعلق بأسرار الدفاع، كما أن المشرع لم يفرق بين الوطني والاجنبي في ارتكاب جريمة التجسس، كما جعل فعل التجسس المرتكب من الموظف ظرفا مشدداً وهو أمر محمود.

وفي إطار الحسابات المالية المصرفية فقد جرم المشرع العراقي التجسس بصورته التقليدية على السرية المصرفية وذلك في المادة (45) من قانون البنك المركزي العراقي رقم 64 لعام 1976 الملغى، بمنع اطلاع الغير على المعلومات الخاصة بالعملاء، حيث نصت على أن "تعتبر كافة المعلومات المتعلقة بأسماء المودعين، ومبالغ ودائعهم وأية معلومات تتعلق بها، وكذلك مبالغ الائتمان والالتزامات غير المباشرة، واسماء العملاء الممنوحة لهم من الامور السرية التي لا يجوز تزويد أية جهة بها، عدا الجهة القضائية المختصة أو الجهات الرسمية الآخرى التي يخولها القانون ذلك"، ويمنع أيضا قانون البنك المركزي رقم 56 لعام 2004 النافذ في المادة (22) منه، كشف أو نشر هذه المعلومات من قبل من حصل عليها بحكم وظيفته حيث نصت على أن "1 - يمنع أي شخص يشغل منصب محافظ أو نائب المحافظ أو عضو في المجلس أو موظف أو وكيل أو مراسل للمصرف المركزي العراقي عن القيام بما يلي: أ - السماح للآخرين بالاطلاع على معلومات خاصة غير متاحة للعموم أو الكشف عنها أو نشرها يكون قد حصل عليها أثناء تأدية مهام وظيفته الرسمية، الا إذا طلب منه ذلك وفقا للفقرة (2) من هده المادة...، 2 - يجوز للمصرف المركزي العراقي أن يتبادل المعلومات المتعلقة بالإشراف....، ويجوز أن تتضمن هذه المعلومات المتبادلة معلومات سرية بشرط إقتناع المصرف المركزي العراقي أن الخطوات اللازمة للحفاظ على سرية هذه المعلومات قد أتخذت".

أما عن مشروع قانون الجرائم المعلوماتية العراقي لعام 2012 فقد تضمنت المادة (3) تجريم الدخول أو البقاء غير المشروع حيث نصت على أن " أ - الدخول أو البقاء أو اتصال غير المشروع مع كل أو جزء من تقنية المعلومات أو الاستمرار به. ب - محو أو تعديل أو تشوية أو نسخ أو نقل أو تدمير للبيانات المحفوظة وللأجهزة والانظمة الالكترونية وشبكات الاتصال والحاق الضرر بالمشتركين والمستفيدين. ج - الحصول على معلومات حكومية سرية "، وردت في النص عبارة " تقنية المعلومات" فقط، و الافضل إيراد عبارة " النظم المعلوماتية أو الشبكة المعلوماتية أو المواقع الالكترونية أو غيرها من الوسائل التقنية "، يضاف إلى ذلك اشتراط النص لتحقق الجريمة أن يكون هنالك إعتداء على " البيانات المحفوظة والانظمة الالكترونية وشبكات الاتصال "، والافضل استخدام عبارة " أو" بدل من عبارة " و " لأن الاعتداء على أحدها يكفي لقيام جريمة، كما أن عبارة " والحاق الضرر بالمشتركين والمستفيدين"، لم تكن دقيقة لأن جريمة التجسس هي من جرائم الخطر وتجرم حتى لو لم يكن هنالك ضرر، لتوفر الحماية للبيانات أو المعلومات أو غيرها من أي إنتهاك لسريتها.

كما ورد في النص عبارة " الحصول على معلومات حكومية سرية" ماذا يراد بها هل هي ظرف مشدد أم ماذا، ومن الجدير بالاشارة أن مشروع قانون الجرائم المعلوماتية لعام 2012 قد خلا من أحكام عقابية حيث وردت (الاحكام العقابية بحاجة الى دراسة من القانونيين) وبالتالي يكون النص المقترح " 1 - يعاقب بالسجن والغرامة التي لا تزيد عن عشرة ملايين أو بأحدى هاتين العقوبتين، كل من دخل أو اتصل أو اعترض دون تصريح أو تجاوز التصريح الممنوح له، في موقع الكتروني أو نظام معلوماتي أو شبكة معلوماتية أو أية وسيلة تقنية أخرى، في كل أو جزء منها، باستخدام وسائل التقنية، وتكون العقوبة السجن مدة لا تقل عن سبعة سنوات والغرامة التي لاتقل عن عشرة ملايين أو باحدى هاتين العقوبتين،

أذا ترتب على ذلك محو أو تعديل أو تشوية أو نسخ أو نقل أو إفشاء أو نشر أو تسجيل أو تدمير للبيانات أو البرامج المحفوظة أو للأجهزة أو الانظمة الالكترونية أو شبكات الاتصال أو غير ذلك، سواء كانت تابعة للمؤسسات الاقتصادية أو التجارية أو المالية أو الصناعية أو العلمية أو المشتركين أو المستفيدين. 2 - تكون العقوبة السجن المؤبد أو المؤقت و الغرامة إذا حصل الجاني على بيانات أو معلومات حكومية سرية أو مايعتبر كذلك".

كما جرمت المادة (4) الاعتراض غير المشروع حيث نصت على أن "الاعتراض المتعمد بدون وجه حق لخط سير البيانات بأي من الوسائل الفنية وقطع بث أو أستقبال بيانات تقنية المعلومات"، ورد بالنص لفظ " المتعمد" وهي زائدة فالاعتراض لا يقع إلا عمدا، كما وردت عبارة "وسائل فنية" غير دقيقة لأنها غالبا تأتي للدلالة على الصياغة السهلة للكلام أو على الاعمال الرفيعة[1] كما تأتي للدلالة على ما يكون له قيمة فنية ثمينة كالتحف[2]، والادق أستخدام عبارة " وسائل تقنية" فهي مرادفة لكلمة تكنولوجيا، كما أن التقنية تأتي على وزن (علمية) وهي مصدر صناعي من التقن بوزن (العلم)[3]، كما أنتقد النص المتقدم لعدم إيراده للصور الاخرى للتجسس كما فعلت القوانين المقارنة كالتشريع السعودي والاماراتي، كما أن النص لم يوضح هل كل اعتراض مجرم، وما هو الوضع القانوني للاعتراض الذي يقع تنفيذا للقانون لذلك اقترحنا إعادة الصياغة على النحو الاتي "يعاقب بالحبس والغرامة التي لا تقل عن مليون دينار أو بأحدى هاتين العقوبتين، كل من اعترض أو التقط أو تنصت بدون تصريح أو تجاوز التصريح الممنوح له، لخط سير البيانات

(1) عبد الرحمن حسن حبنكة الميداني، البلاغة العربية أساسها وعلومها وفنونها، ج1، ط1، دار القلم، دمشق، 1996، ص 18 - 21.

(2) إبراهيم مصطفى وآخرون، مرجع سابق، ج1، ص 173.

(3) بكر بن عبد الله أبو زيد، معجم المناهي اللفظية ويليه فوائد في الالفاظ، ج21، ط3، دار العاصمة، الرياض، 1996، ص 404.

أو المعلومات أو الاتصالات أو الصور أو غير ذلك، وتكون العقوبة هي الحبس لمدة لا تقل عن ثلاث سنوات و الغرامة التي لا تقل عن ثلاثة ملايين أو إحدى هاتين العقوبتين، إذا ترتب عن ذلك أفشاء أو كشف أو إذاعة أو نقل أو تسجيل أو نشر لتلك البيانات أو المعلومات أو الاتصالات أو الصور أو غير ذلك".

وجرمت المادة (5) " الدخول واعتراض الشبكات الحرجة للدولة، حيث نصت على أن "جريمة الدخول واعتراض الشبكات الحرجة للدولة: أ - أتلف أو عيب أو أعاقة اجهزة أو أنظمة أو برامج أو شبكات المعلوماتية التابعة للجهات الامنية أو العسكرية أو الاستخباراتية بقصد المساس بأمن الدولة الداخلي أو الخارجي أو تعريضها للخطر. ب - استخدام عمدا أجهزة الحاسوب وبرامجه أو أنظمته أو شبكة المعلومات التابعة للجهات الامنية أو العسكرية أو الاستخبارية، بقصد الاضرار بها أو النسخ منها أو بقصد إرسال محتواها لجهة معادية أو الاستفادة منها في جرائم ضد أمن الدولة الداخلي أو الخارجي، أو تسهيل إخفاء معالم تلك الجرائم أو تغطيتها"، يلاحظ على النص أنه مبتورٌ لم يتطرق الى السلوك الاجرامي كأن يقال "كل من دخل أو اعترض"، كما لم يبين إلى أي شيء يتم الدخول إليه واعتراضه، هل هي الأنظمة المعلوماتية أو الشبكات...الخ، حيث ورد بالنص عبارة أتلف أو عيب غير واضحه هل القصد منها الاتلاف أو التعيب المادي، كما انتقد ورود عبارة "الدخول واعتراض الشبكات الحرجة للدولة" وذلك لأن الدخول يختلف عن الاعتراض وكلاهما مجرم ولايشترط تحققهما معا من أجل تجريم الفعل، كما أن عبارة الشبكات الحرجة، عبارة غامضة تثير اللبس والافضل استخدام عبارة "الدخول أو اعتراض الشبكات أو المواقع الالكترونية أو النظم المعلوماتية أو أية من وسائل التقنية الحكومية أو المستخدمة من قبل الحكومة أو تؤدي عملا لخدمة الحكومة"، كما يأخذ على النص اشتراطه قصداً خاصا هو " المساس بأمن الدولة الداخلي أو الخارجي أو تعريضها للخطر أو استخدام عمدا أجهزة الحاسوب

وبرامجه أو أنظمته أو شبكة المعلومات التابعة للجهات الامنية أو العسكرية أو الاستخبارية بقصد الاضرار بها أو النسخ منها أو بقصد إرسال محتواها لجهة معادية أو الاستفادة منها في جرائم ضد أمن الدولة الداخلي أو الخارجي، أو تسهيل إخفاء معالم تلك الجرائم أو تغطيتها"، في حين أن جريمة التجسس يكفي لتحققها القصد الجرمي العام، كما أن عبارة " الجهات الاستخباراتية " زائدة لا مبرر لذكرها لأنها إحدى الأجهزة الأمنية، والصياغة المقترحة هي "1 - يعاقب بالسجن والغرامة، كل من اعترض أو التقط أو تنصت أو دخل بغير تصريح أو تجاوز التصريح الممنوح له، إلى موقع الكتروني، أو نظام معلوماتي الكتروني، أو شبكة معلوماتية، أو أيا من الوسائل التقنية، باستخدام وسائل تقنية المعلومات. 2 - وتكون العقوبة هي السجن مدة لا تقل عن عشرة سنوات والغرامة، إذا نتج عن ذلك إتلاف أو عيب أو إعاقه أو إطلاع أو نسخ أو تسجيل أو إذاعة أو كشف أو أفشاء أو نشر أو تسليم للبيانات أو المعلومات أو الانظمة الالكترونية أو المواقع الالكترونية أو الشبكات الحكومية أو ما يعتبر كذلك". كما جرمت الفقرتين (د، ز) من المادة (7) الاعتداء على سلامة بيانات التوقيع الالكتروني أو الرسائل الالكترونية أو المعلومات أو المحررات من خطر الإفشاء أو الاختراق أو الاعتراض، حيث نصت على أن " د - كل من علم بحكم عمله ببيانات التوقيع أو الرسائل الالكترونية أو المعلومات فأفشاها بقصد الاضرار بالغير أو تحقيق منفعة مالية له أو لغيره أو استخدمها في غير الغرض الذي قدمت من أجله. ه - توصل بأي وسيلة إلى الحصول بغير حق على توقيع أو وسيلة أو محرر ألكتروني أو اختراق هذه الوسيلة أو اعتراضها أو عطلها عن أداء دورها"، جاءت الفقره (ه) دون تحديد وسيلة لإرتكاب الجريمة وهو أمر جيد، ولكن يأخذ على الفقرة (د) اشتراطها القصد الجرمي الخاص حيث يكفي القصد الجرمي العام، ونقترح تعديل (الفقرة د من المادة 7) على النحو الآتي "يعاقب بالحبس والغرامة التي لا تقل عن ثلاثة ملايين دينار أو بأحدى هاتين العقوبتين، كل من علم بحكم عمله ببيانات التوقيع الالكتروني

أو الرسائل الالكترونية أو المعلومات فإفشاها للغير أو قام بنشرها أو نسخها أو تسجيلها أو حذفها أو إتلافها أو استخدامها في غير الغرض الذي قدمت من أجله". وجرمت المادة (14) الاعتداء على الحياة الخاصة حيث نصت على أن "د – دخل عمدا بدون تصريح موقعا أو نظاما معلوماتيا أو اتصل مع نظام الحاسب أو جزء منه. ه – استخدم أو تسبب دون تصريح في استخدام الحاسب العائد للغير بطريقة مباشرة أو غير مباشرة. و – حذف أو تدمير أو تغيير أو تعييب أو تعطيل أو إعادة نشر بيانات ومعلومات تعود للغير بغير وجه حق. ز – إلتقط أو اعترض بغير وجه حق ما هو مرسل عن طريق احدى أجهزة الحاسوب أو شبكة المعلومات لاستخدامها في تحقيق منفعة مالية له أو لغيره ". جاءت صياغة هذة الفقرات ركيكة ونقترح الصياغة الاتية " يعاقب بالحبس مدة لا تقل عن ستة أشهر والغرامة التي لا تقل عن مليون دينار ولا تزيد عن سبعة ملايين أو بإحدى هاتين العقوبتين، كل من استخدم شبكة معلوماتية، أو نظام معلوماتي ألكتروني، أو إحدى وسائل تقنية المعلومات، في الاعتداء على خصوصية شخص في غير الاحوال المصرح بها قانونا بإحدى الافعال الآتية: د – كل من دخل أو اتصل أو اعترض، النظام المعلوماتي أو موقع الكتروني أو شبكة معلوماتية أو أية من الوسائل التقنية، دون تصريح أو بتجاوز التصريح الممنوح له، وترتب على ذلك اعتداءً على الحياة الخاصة للشخص نفسه أو لعائلته. ه – استراق السمع أو اعتراض أو تسجيل أو نقل أو بث أو إفشاء محادثات أو اتصالات ومواد صوتية أو مرئية أو استخدام حاسب عائدٍ للغير بصورة مباشرة أو غير مباشرة. و – التقاط صور للغير أو إعداد صور الكترونية أو نقلها أو كشفها أو حذفها أو تعييبها أو إعادة نشرها أو نسخها أو الاحتفاظ بها. ز – التقط أو اعترض أو نشر أخبار أو صور الكترونية أو صور فوتوغرافية أو مشاهد أو تعليقات أو بيانات أو معلومات ولو كانت صحيحة وحقيقية دون تصريح أو تجاوز التصريح الممنوح له. كما يعاقب بالحبس مدة لا تقل عن سنة واحدة والغرامة التي لا تقل ثلاثة ملايين دينار ولا تزيد عن عشرة ملايين دينار أو بأحدى هاتين العقوبتين، كل من استخدم

نظام معلوماتي الكتروني، أو إحدى وسائل تقنية المعلومات، لإجراء أي تعديل أو معالجة على تسجيل أو صورة أو مشهد، بقصد التشهير أو الاساءة إلى شخص آخر، أو الاعتداء على خصوصيته أو انتهاكها".

نخلص مما تقدم أن جريمة التجسس مجرمة في جميع الدول بمختلف صورها ولا يمكن ممارستها الا وفقاً للقانون أو لضرورة أمنية كما في التشريع الامريكي والدستور العراقي لعام 2005 مثلا، كما أن التجسس يستهدف جميع القطاعات بالدولة أو القطاع الخاص أو الأفراد، كما تتفق أغلب الدول على تشديد العقاب إذا كان الاعتداء واقعا على البيانات أو الأنظمة أو المواقع الالكترونية أو الشبكات الحكومية أو ماتعتبر كذلك، وبعضها يشترط قصدا جرمياً خاصاً وبعضها لا يشترط، ونرى كذلك أن التجسس بصورة عامة متجدد في الافعال المرتكبة أو الوسائل المستخدمة، ودليلنا على ذلك التشريع الاماراتي الخاص بمكافحة جرائم تقنية المعلومات، حيث أنه صدر في عام 2006 وتم إلغاءه واصدار قانون جديد في عام 2012، حيث تمت إضافة صور أخرى لافعال التجسس وخاصة في إطار الحياة الخاصة، كاستراق السمع أو تسجيل أو نقل أو بث أو إفشاء محادثات أو اتصالات ومواد صوتية أو مرئية...الخ.

أخيرا أدعُ المشرع العراقي الى سن تشريع يجرم كافة صور التجسس كالدخول غير المشروع أو إلتقاط البيانات أو اعتراضها أو التنصت عليها...الخ، تحقيقا لمبدأ الشرعية وعوناً للسلطة القضائية في تحقيق العدالة، مهتديا بالاتفاقات الدولية، وعلى غرار التشريعات العربية الخاصة بالتجسس المعلوماتي.

المبحث الثاني

طبيعة جريمة التجسس المعلوماتي ونطاقها

سنبين في هذا المبحث طبيعة الجريمة ونطاقها وذلك في مطلبين وعلى النحو الآتي:

- **المطلب الاول:** طبيعة جريمة التجسس المعلوماتي.
- **المطلب الثاني:** نطاق جريمة التجسس المعلوماتي.

المطلب الاول

طبيعة جريمة التجسس المعلوماتي

سنتناول في هذا المطلب طبيعة جريمة التجسس المعلوماتي وذلك في فرعين وعلى النحو الاتي:

- **الفرع الاول:** جريمة التجسس جريمة سياسية.
- **الفرع الثاني:** جريمة التجسس المعلوماتي جريمة أمن دولة خارجي.

الفرع الاول

جريمة التجسس جريمة سياسية

تناولت عدة مذاهب مفهوم الجريمة السياسية، ومنها المذهب الشخصي الذي يعد من أول المذاهب التي جاءت لتحديد مفهوم الجريمة السياسية، واعتمد في ذلك على الباعث أو القصد في ارتكاب الجريمة، اي الغرض الذي يريد مرتكب الجريمة الوصول اليه، دون التقيد بموضوع الجريمة أو طبيعة الحق المعتدى عليه[1]، وقد عرف اصحاب هذا المذهب الجريمة السياسية بأنها(الجريمة التي يكون الباعث عليها و الغرض الوحيد فيها، محاولة تغير النظام السياسي وتبديله أو قلبه)[2]، استنادا لما تقدم أرى أن جريمة التجسس ممكن أن تكون سياسية إذا كان الباعث على أرتكابها التجسس لصالح المعارضة مثلا من أجل قلب نظام حكم في دولة معينة، وقد تعرض هذا المذهب للنقد بحجة، أن الباعث ليس ركنا من أركان الجريمة وهو أمر خارج عنها، كما ان القوانين العقابية لا تعير أهمية للباعث على ارتكاب الجريمة، اللهم إلا في سلطة القاضي التقديرية... الخ[3].

أما عن المذهب الموضوعي، فقد جاء على خلاف ما جاء به المذهب الشخصي، حيث استندوا إلى ماديات الحق المعتدى عليه، فالجريمة السياسية هي التي يكون موضوعها الاعتداء على مصلحة أو حق سياسي للفرد أو النظام السياسي للدولة، وبهذا المعيار أخذ مؤتمر كوبنهاجن لعام 1935 [4].

(1) د. سعد ابراهيم الاعظمي، جرائم التجسس....، مرجع سابق، ص 56.

(2) د. وداد عبد الرحمن القيسي، الجريمة السياسية في القوانين المقارنة، متاح على الموقع - www.justice lawhome.com. وقت وتاريخ الزيارة 2100، 22/10/ 2015

(3) للمزيد: د. منتظر سعيد حمودة، مرجع سابق، ص 106 ومابعدها.

(4) د. حسام علي عبد الخالق الشيخة، المسؤولية والعقاب على جرائم الحرب، دار الجامعة الجديدة للنشر، القاهرة، 2004، ص 81 - 82.

وعرف أصحاب هذا المذهب الجريمة السياسية على أنها (هي الجرائم التي تنطوي على معنى الاعتداء على نظام الدولة السياسي، سواء من جهة الخارج، أي المساس باستقلالها أو سيادتها، أو من جهة الداخل، أي المساس بشكل الحكومة أونظام السلطة العامة أو حقوق الافراد الساسية)[1]، وهنا أيضا يمكننا القول إن جريمة التجسس جريمة سياسية بإعتبار أنها من الجرائم الماسة بأمن الدول من جهة الخارج، إلا أن هذا المذهب لم ينجوا من الانتقاد ايضا، بحجة أنه يؤدي إلى التشديد على الخصوم السياسين، وأنه يهدف إلى حماية نظام الحكم القائم دون النظر إلى دوافع المجرم السياسية، كما أنه ينظر إلى الركن المادي دون الركن المعنوي المتمثل بشرف الباعث ونبل المقصد...الخ [2].

وقد اعتبر المذهبان جريمة التجسس من الجرائم السياسية البحتة، سواء بالنظر الى الباعث على ارتكابها، أو بالنظر إلى الحق المعتدى عليه، ومن الجرائم التي تلحق ضرراً أو خطراً بالصالح العام، ولا تلحق ضررا بحق من حقوق الافراد[3]، وأستناداً الى ما تقدم فقد تم تعريف الجريمة السياسية البحتة من غالبية الفقه بأنها(الجرائم التي تكتسب صفة السياسية بالنظر إلى الباعث على ارتكابها، أو لطبيعة الحق المعتدى عليه فيها، وهي جرائم الاعتداء على السلطة السياسية في الدولة سواء من الخارج أو من الداخل)[4].

---

(1) د. محمد عزت سلام، الجريمة السياسية في ظل النظام العالمي الجديد، منشأة المعارف، الاسكندرية، 2013، ص 59.

(2) للمزيد: محمد علي السير، في الجريمة السياسية، منشورات الحلبي الحقوقية، بيروت، 2003، ص 44 - 45.

(3) د. مجدي محمود محب حافظ، موسوعة جرائم الخيانة والتجسس، ط 1، المركز القومي للاصدارات القانونية، القاهرة، 2007، ص 110 - 111. أسامة أحمد محمد سمور، الجرائم السياسية في التشريع الجنائي الاسلامي (دراسة فقهية مقارنة)، رسالة ماجستير، جامعة النجاح الوطنية، فلسطين، 2009، ص 152.

(4) د. منتصر سعيد حمودة، مرجع سابق، ص 165.

يضاف الى ما تقدم ظهر مذهب آخر هو المذهب التوفيقي(المختلط)، نتيجة للانتقادات التي وجهت للمذهبين الشخصي والموضوعي، والذي جاء محاولا الجمع بين مزايا المذهبين السابقين وتجنب عيوبها، و وجد أن الاعتماد على مذهب واحد يؤدي الى ما يسمى ظاهرة تسييس الجريمة، والتي تعني سيادة التشديد بالعقاب مع المجرم السياسي، حيث يؤدي اعتناق المذهب الشخصي الى التوسيع نطاق الجريمة السياسية، فيما اذ تم أعتناق المذهب الموضوعي فإن ذلك يؤدي إلى أن تسود النظرية العقابية المخففة، وبالتالي تضيق من نطاق الجريمة السياسية، وعليه اعتمد المعياران الشخصي والموضوعي معا، لانه المعيار العلمي الذي يجمع بين المصالح الاجتماعية، ويهدف الى حماية الحقوق والحريات الفردية[(1)]. وقد أخذ المشرع العراقي في قانون العقوبات بالمذهبين الشخصي والموضوعي في تحديد مفهوم الجريمة السياسية والذي استثنى فيه جريمة التجسس من نطاق الجرائم السياسية[(2)]، وفي حال عدم تبني المشرع الجنائي اتجاها في تحديد مفهوم الجريمة السياسية، تنكر الجهات القضائية الصفة السياسية رغم وجودها[(3)].

ويترتب على اعتبار الجريمة المرتكبة جريمة سياسية، عدة نتائج فمن حيث العقاب، الغيت عقوبة الاعدام من قبل أغلب دول العالم في الجرائم الساسية[(4)]،

(1) محمد عزة سلام، مرجع سابق، ص 62.

(2) عرفت المادة (21) من قانون العقوبات العراقي الجريمة السياسية بأنها (هي الجريمة التي ترتكب بباعث سياسي أو تقع على الحقوق الساسية العامة أو الفردية. وفيما عدا ذلك تعتبر الجريمة عادية. ومع ذلك لاتعتبر الجرائم التالية سياسية ولو قد أرتكبت بباعث سياسي...2 – الجرائم الماسة بأمن الدولة الخارجي).

(3) ففي قرار لمحكمة النقض المصرية رقم 375 الصادر في 7 يوليو عام 1953، تبنت المذهب الشخصي، و أنكرت الصفة السياسية للجريمة التي موضوعها متعلق بالعملية الانتخابية بحجة أنها وقعت لغرض غير سياسي، في حين تبنت المذهب الموضوعي في حكم أخر حيث أعتبرت جريمة تجمهر وقعت لمناصرة لأحد المرشحين في الانتخابات ضد منافسية جريمة سياسية في قرار لها في 7 يوليو من نفس العام رقم القرار381. وهو مايعكس تخبط القضاء في حال عدم تبني المشرع موقف واضح.أشار اليه: د. محمد عزت سلام، مرجع سابق، ص 56 وما بعدها.

(4) د منتظر سعيد حمودة، مرجع نفسه، ص 258.

أما عن الاختصاص والاجـراءات تخضع بعض الـدول الجـرائم السياسية إلى نظام خاص من حيث الاختصاص ومن حيث الاجراءات[1]، أما عن نظام تسليم المجرمين، فإن من المبادئ التي تكاد تكون مستقرة في دساتير الدول وتشريعاتها، مبدأ عدم تسليم المجرمين (حق اللجوء السياسي) [2].

ومـن التشـريعات التـي اعـتبرت جـريمـة التجسس بصورتيها التقليدية والمعلوماتية سياسية، المشرع الفرنسي وهو من المشرعين القلائل الذين اضفوا الطابع السياسي على جريمة التجسس التقليدية وبمواقف متباينة، انتهت إلى اعتبار جريمة التجسس من الجريمة السياسية، حيث كانت جرائم أمن الدولة من جهة الخارج في فرنسا ومنذ عام 1810 توصف بالصفة السياسية، وتأكد ذلك بإلغاء عقوبة الاعدام بدستور [3]1848، واستمر ذلك حتى صدور قانون 1939.

حيث نصت (الفقرة 4 من المادة 84) (تعتبر جرائم الاعتداء على أمن الدولة من جهة الخارج من جرائم القانون العام)، وبالنص المتقدم نزعة الصفة السياسية، عن جريمة التجسس وعوملت معاملة الجرائم العادية[4]، ولكن وبعد تعدد اشكال الاعتداء على أمن الدولة من جهة الخارج، وظهور تيارات تدعوا إلى نزع الصفة السياسية عن جرائم أمن الدولة، جاء قانون 1960 حاسما بأضافة الصفة السياسية على جرائم أمن الدولة من جهة الخارج[5]، كما نبين أن المشرع الفرنسي وضع معياراً جنسية الفاعل في تحديد نوع الجريمة، حيث إذا كان مفشي الاسرار أجنبي فهو جاسوس واذا كان وطني فهو خائن[6].

(1) د. محمود ابراهيم اللبيدي، الحماية الجنائية لأمن الدولة، دار شتات، القاهرة، 2009، ص 102. د. مجدي محمود محب حافظ، مرجع سابق، ص 123.

(2) د. محمد عزت سلام، مرجع سابق، ص 54. د. حسام علي عبد الخالق الشيخة، مرجع سابق، ص 83.

(3) د. محمود ابراهيم اللبيدي، مرجع سابق، ص 106.

(4) د. عبد الحميد الشواربي، الجرائم السياسية، ط 2، منشأة المعارف، الاسكندرية، 1999، ص 39.

(5) د. ابراهيم محمد اللبيدي، مرجع سابق، ص 130.

(6) د. مجدي محمود محب حافظ، مرجع سابق، ص 319.

واستنادا لما تقدم نخلص إلى أن جريمة التجسس بصورة عامة والتجسس المعلوماتي بصفه خاصة في التشريع الفرنسي هي جريمة سياسية، وأستند في ذلك لنص (الفقرة 6 من المادة411) من قانون العقوبات الفرنسي الجديد التي أوردت عقوبة الاعتقال لجريمة التجسس والتي قد تستهدف معطيات مبرمجة آليا حيث نصت على أن "يعاقب بالاعتقال لمدة خمسة عشر سنة... كل من سلم الى دولة أجنبية أو لمشروع أو منظمة أجنبية أو لأي جهة تخضع لسيطرة أجنبية أو لأحد عملائها، أو مهد في سبيل ذلك، معلومات، أساليب، أشياء، وثائق، معطيات مبرمجة آليا، أو فهارس، أذا كان في استعمالها أو إفشاءها أو تجميعها مايشكل بطبيعته ضرراً بالمصالح الاساسية بالامة" كما لم يحدد التشريع الفرنسي وسيلة معينه لإرتكاب جريمة التجسس المعلوماتي.

أما المشرع الاردني فإنه استند الى ما استقر عليه الفقه من اعتبار جرائم أمن الدولة الخارجي والجرائم الماسة بالقانون الدولي والتجسس والجرائم الواقعة على أمن الدولة الداخلي جرائم سياسية، وحدد على ضوء ما استقر عليه الفقه عقوبات هذة الجرائم، بموجب المواد (102 - 143) من قانون العقوبات الاردني رقم 58 لسنة [1] 1951. إلا أنه نجد موقفاً مغايرا في قانون العقوبات العسكري، من جريمة التجسس حيث عاقب القانون المذكور بالاعدام على افشاء كلمة السر أو كلمة المرور أو الاشارة الجوابية، وهي عقوبه لا تنفذ بحق من يرتكب جريمة سياسية[2].

(1) د.عبد الحميد الشواربي، مرجع سابق، ص 41.

(2) المادة (38) من قانون العقوبات العسكري الاردني رقم 30 لعام 2002.

الفرع الثاني

جريمة التجسس المعلوماتي جريمة أمن دولة خارجي

تعد جريمة التجسس من الجرائم الجنائية التي تهدد أمن الدولة الخارجي، حيث يكون في الواقعة المكونة للجريمة مساس بأمن الدولة الخارجي لا بشخص من الاشخاص[1]، ولخطورة جريمة التجسس في زمن الحرب وما بعدها دفع فقهاء القانون الجنائي إلى نزع الصفة السياسية عنها، وجعل الدول تعامل مع مرتكبيها بالقسوة وفرض عقوبة الاعدام عليهم[2]، وترتكب هذة الجرائم في الغالب من قبل أفراد أو مجموعة أفراد، تأخذ شكل شبكات أو تنظيمات محددة[3]، ولجرائم أمن الدولة الخارجي عدة ميزات منها.

تمتاز جرائم أمن الدولة من جهة الخارج بعدة خصائص، حيث تعد حقيقة متغيرة ونسبية، فهي نسبية لاختلاف المصالح الأمنية لدى الدول، وتعتبر متغيرة لارتباط أمن الدولة باعتبارات مختلفة، كعلاقة الدولة بالدول المجاورة والمجتمع الدولي[4]، وتتميز أيضا بدناءة وانحطاط الباعث على ارتكابها[5] حيث يدفعهم الى ارتكابها الانانية والمال[6]، أما عن المصلحة المحمية في جرائم أمن الدولة

(1) محمد علي السير، مرجع سابق، ص 91.

(2) المادة (158) قانون عقوبات العراقي. سعد ابراهيم الاعظمي، جرائم التجسس...، مرجع سابق، ص 58.

(3) د. سعد ابراهيم الاعظمي، الجرائم الماسة بأمن الدولة الداخلي، ط 1، دار الشؤون الثقافية العامة، بغداد، 1989، ص 40.

(4) للمزيد: د. محمود ابراهيم اللبيدي، مرجع سابق، ص 24.

(5) د. سعد ابراهيم الاعظمي، جرائم التجسس...، مرجع سابق، ص 61.

(6) عباس منعم صالح، الحماية الجنائية لأمن الدولة الداخلي، رسالة ماجستير، الجامعة المستنصرية كلية القانون، 2012، ص 44.

الخارجي، فهو كيان الدولة بأسره والمتمثل باستقلال وسلامة وسيادة ووحدة أراضيها[1]، أذ لا يقف تأثيرها على الحكومة فقط، بل يمتد ضررها الى الامة[2] و تهدد وجود الدولة أو اقتطاع جزء من اراضيها[3]، كما تعد من جرائم الخطر والتي لا يتطلب المشرع فيها حصول الضرر، بل يكفي ارتكاب الفعل الذي فيه مساس بالمصلحة المحمية[4]، ولها سياسة تشريعية خاصة حيث تتميز القواعد التشريعية بالصياغة الحرة و بالقسوة، إذ يتم التوسع في الظروف المشددة و أفعال الإشتراك[5] لتشمل الشخص الذي لا يعد شريكا وفقا للقواعد العامة لعدم وقوع الجريمة[6]، كما يتغير وصف الجريمة من جنحة الى جناية لجريمة التجسس المرتكبة في زمن الحرب في فرنسا مثلا[7]، و لجرائم أمن الدولة سياسة إجرائية خاصة[8] حيث يكون النظر فيها من قبل محاكم عسكرية[9] أو محاكم خاصة، ففي فرنسا مثلا تختص بنظرها محاكم أمن الدولة في زمن السلم، والمحاكم العسكرية في زمن الحرب[10]، كما خص المشرع العراقي جرائم أمن الدولة الخارجي (التجسس)

---

(1) فهد عيسى ناصر بن صليهم، مبدأ العينية واثرة في مكافحة الجرائم العابرة للحدود الدولية دراسة مقارنة، رسالة ماجستير، جامعة نايف العربية للعوم الامنية، الرياض، 2009، ص 154.

(2) د. منتظر سعيد حمودة، مرجع سابق، ص 126 وما بعدها. د. محمد عزت سلام، مرجع سابق، ص 129.

(3) د. سعد ابراهيم الاعظمي، الجرائم الماسة...، ص 28.

(4) د. محمد ابراهيم اللبيدي، مرجع سابق، ص 25.

(5) للمزيد: د. محمود ابراهيم اللبيدي، مرجع نفسة، ص 26.

(6) في مصر تسري احكام المواد (82، 83، 95، 96، 97 و 98)من قانون العقوبات المصري استثاءا من تطبيق المادة (40) وهي قاعدة عامة خاصة بالاشتراك. للمزيد: د. تامر احمد عزات، الحماية الجنائية لأمن الدولة من جهة الخارج (دراسة موضوعية أجرائية مقارنة)، ط2، دار النهضة العرابية، القاهرة، 2007، ص78.

(7) د. منتظر سعيد حمودة، مرجع سابق ص 129.

(8) د. محمد هشام أبو الفتوح، قضاء أمن الدولة، دار النهضة العربية، القاهرة، 1996، ص 386 ومابعدها. فهد عيسى ناصر بن صليهم، مرجع سابق، ص 159.

(9) محمد علي السير، مرجع سابق، ص 96.

(10) د. مجدي محب حافظ، مرجع سابق، ص 123.

بمحكمة خاصة أيضا ألا وهي محكمة الثورة[1] الملغاة، كما يتميز الركن المادي والمعنوي في جرائم أمن الدولة الخارجي بكون طبيعة أفعالها تعد مادية في جانب ومعنوية في جانب آخر، كالتخابر أو السعي لدى دولة أجنبية[2].

وتأسيساً على ما تقدم فإن جرائم أمن الدولة الخارجي تعرف من ناحية سياسية بأنها(هي كيان الدولة المادي والمعنوي تجاه الدول الأخرى، وفقدان الدولة لهذا الكيان يعني انهيار ذاتيتها المميزة للشعب وصيرورته ذليلا لغيره، بمعنى انهاء الشخصية الدولية للدولة)[3]. كما تعرف من ناحية قانونية بأنها (الأفعال المجرمة التي تقع على الدولة في علاقاتها بالدول الأخرى، ويراد بها الاعتداء على استقلالها وزعزعة كيانها و إعانة عدوها على غزو البلاد)[4].

وأما موقف التشريعات من جريمة التجسس بصورتها المعلوماتية أو التقليدية، كونها من جرائم أمن الدولة الخارجي، فبالنسبة للتشريع الأمريكي اعتبر جريمة التجسس التقليدية من جرائم أمن الدولة الخارجي والتي تناولها في الفصل السابع والثلاثون من قانون العقوبات الامريكي[5].

وذلك في المادة (794) حيث جرمت فعل جمع أو تسليم معلومات دفاعية لمساعدة دولة أجنبية إذ نصت على أن "يعاقب بالاعدام....كل من يقوم بقصد الاضرار بالولايات المتحدة الامريكية أو لمصلحة دولة أجنبية بالاتصال أو بتسليم او بنقل اية وثيقة...أو أجهزة أو معلومات تتعلق بالامن القومي....''، أما عن

(1) د. سعد ابراهيم الاعظمي، جرائم التجسس....، مرجع سابق، ص 286.

(2) د. سعد ابراهيم الاعظمي، الجرائم الماسة....، مرجع نفسه، ص 18 وما بعدها.

(3) د. محمود ابراهيم اللبيدي، مرجع سابق، ص 5.

(4) د. تامر أحمد عزات، مرجع سابق، ص 57.

(5) أشارة اليها: د. مجدي محب حافظ، مرجع سابق، ص 443 وما بعدها. د. أيمن عبد الحفيظ عبد الحميد سليمان، مرجع سابق، ص 163 - 164.

جريمة التجسس المعلوماتي المنصوص عليها في المادة (1030) من قانون إساءة استخدام الحاسب جرمت الدخول غير المشروع الى حواسيب الحكومة الامريكية أو التي تتعلق بعمل الحكومة سواء كانت مالية أو اقتصادية أو الاتصالات التي تتم داخل الولايات المتحدة أو خارجها أو تجاوز التصريح الممنوح[1].

أما التشريعات العربية فبالنسبة للتشريع السعودي فإنه عاقب على جريمة افشاء الاسرار العسكرية والقوات الحربية، بالقتل أو الصلب...الخ[2]، وعليه فهو يأكد لنا بعدم اعتبار جريمة التجسس جريمة سياسية، إضافة إلى أن نظام مكافحة الجرائم المعلوماتية السعودي جاء واضحا في اعتبار جريمة التجسس من جرائم أمن الدولة الخارجي بنص المادة (7) منه.

أما التشريع الاماراتي فإن مرسوم مكافحة جرائم التقنية لعام 2012، اعتبر العديد من الجرائم هي من جرائم أمن الدولة بنص المادة (44) حيث نصت على "تعتبر الجرائم الواردة في المواد (4، 24، 26، 28، 29، 30، 38) من هذا المرسوم بقانون من الجرائم الماسة بأمن الدولة. كما تعتبر من الجرائم الماسة بأمن الدولة، اي جريمة منصوص عليها في هذا المرسوم بقانون إذا ارتكبت لحساب أو لمصلحة دولة أجنبية، أو أي جماعة ارهابية..."، نجد المشرع الاماراتي قد توسع في مفهوم جرائم أمن الدولة حيث اعتبر أي جريمة في هذا المرسوم بقانون ترتكب لمصلحة دولة أجنبية أو إرهابية من جرائم أمن الدولة.

أما التشريع العراقي فأنه قد حذا حذو التشريعات الحديثة والتي جردت جرائم أمن الدولة الخارجي ومنها جريمة التجسس التقليدية من الصفة السياسية، وذلك بموجب (الفقرة أ من المادة 21) من قانون العقوبات العراقي، كما لم يفرق المشرع العراقي بين المواطن والأجنبي في ارتكاب جريمة التجسس، وهو اتجاه

(1) د. حسام محمد نبيل الشنراقي، مرجع سابق، ص 144.
(2) منصور بن ناصر العضيلة، مرجع سابق، ص 71.

سليم لأن أساس التجريم هو خطر الفعل ذاته على أمن الدولة وسلامتها لا بتحقق صفة معينة في الجاني[1]، حيث إن من يرتكب جريمة انتهاك أسرار الدفاع يعتبر جاسوسا بغض النظر عن جنسيته، وقد جعل المشرع العراقي ارتكاب التجسس من قبل المكلف بخدمة عامة ظرفا مشدداً[2].

ومن الجدير بالذكر قد منح القضاء العراقي حق اللجوء الى شخص أجنبي تجسس لمصلحة العراق على دولة أجنبية[3]، مستندا إلى قانون اللاجئين السياسين رقم 114 لعام 1959 والذي يعطي اللجوء السياسي للمدني أو العسكري الذي يطلب اللجوء لاسباب سياسية أو عسكرية، وهو موقف في رأينا يتعارض مع قانون العقوبات العراقي والذي يعتبر جريمة التجسس ليست سياسية وبالتالي لا يمنح حق اللجوء السياسي.

نخلص من خلال استعراض موقف التشريعات من جريمة التجسس بصورة عامة، هي جريمة ذات طبيعة خاصة، قد تكون جريمة أمن دولة أو جريمة سياسية أو جريمة عادية، وأرى أن جريمة التجسس المعلوماتي والتي تستهدف البيانات أو المعلومات أو الأنظمة أو البرامج أو المواقع أو الشبكات الحكومية أو مايعد كذلك سواء كانت سياسية أو عسكرية أو أقتصادية...الخ، هي من جرائم أمن الدولة الخارجي، أما جرائم التجسس التي تستهدف القطاع الخاص أو الافراد فهي من الجرائم العادية.

(1) د. سعد ابراهيم الاعظمي، جرائم التجسس...، مرجع سابق، ص 59 - 60.

(2) المادة (177) من قانون العقوبات العراقي.

(3) د. سعد ابراهيم الاعظمي، جرائم التجسس....، مرجع سابق، ص 65 - 66.

المطلب الثاني

نطاق جريمة التجسس المعلوماتي

قد تستهدف جريمة التجسس المعلوماتي، المعلومات العسكرية والسياسية، أو المعلومات الاقتصادية والصناعية والعلمية، أو المعلومات المتعلقة بالحياة الخاصة، وهذا ما سنوضحه في ثلاثة فروع وعلى النحو الاتي:

- **الفرع الاول:** المعلومات العسكرية والسياسية.
- **الفرع الثاني:** المعلومات الاقتصادية و الصناعية و العلمية.
- **الفرع الثالث:** المعلومات المتعلقة بالحياة الخاصة.

الفرع الاول

المعلومات العسكرية والسياسية

أولا: المعلومات العسكرية:

ويقصد بها(الحقائق التي تتعلق باستعداد البلاد العسكري، وكفاياتها الحربية، ووسائل الدفاع عنها، وعملياتها الحربية في البر والبحر والجو، سواء في وقت السلم أو الحرب....)(1).

وتعرف أيضا بأنها (عبارة عن كل المعلومات أو الاشياء أو الفهارس أو الأساليب التي تتعلق بالشؤون العسكرية التي يجب أن تبقى مكتوما عليها، لأعتبارات الدفاع الوطني وسواء كانت هذه الأسرار تمس القوات المسلحة العامة أو الاحتياطية، كما يشمل السر العسكري الكوادر التي تنظم عمل ونشاط تلك القوات في الداخل أو الخارج.....)(2)، وتعتبر المؤسسات العسكرية الأكثر أهمية من بين مؤسسات الدولة، والتي تستخدم المعلومات على نطاق واسع، لذا فهي تعد مجالا خصبا للاختراق والتجسس(3).

وتتضمن المعلومات العسكرية أسرارا يطلق عليها أسرار الدفاع والتي يقصد بها (الأشياء أو الوثائق أو المعلومات التي يجب أن تبقى مكتومة حرصا على سلامة الدولة)، وقد سار المشرع العراقي على ما سار عليه المشرع الفرنسي والمشرع المصري(4)، بتحديد ما يعتبر من أسرار الدفاع.

(1) للمزيد: د. محمد عودة الجبور، الجرائم الواقعة على امن الدولة وجرائم الارهاب، ط 1، دار الثقافة، عمان، 2009، ص 202.

(2) للمزيد: منصور بن ناصرالعضيلة، مرجع سابق، ص 71.

(3) للمزيد: د. حسين بن سعيد الغافري، مرجع سابق، ص 378.

(4) للمزيد: المادة (85) من قانون العقوبات المصري رقم 112 لسنة 1957.

وذلك بنص المادة (188) من قانون العقوبات العراقي حيث نصت على أن "يعتبر من أسرار الدفاع: 1 - المعلومات الحربية والسياسية والاقتصادية والصناعية، التي هي بحكم طبيعتها لا يعلمها إلا الأشخاص الذين لهم صفة في ذلك والتي تقضي مصلحة الدفاع عن البلاد أن تبقى سرية على من عداهم. 2 - المكاتبات والمحررات والوثائق والرسوم والخرائط والتصميمات والصور، وغيرها من الأشياء، التي قد يؤدي كشفها الى إفشاء معلومات مما أشير إليه بالفقرة السابقة والتي تقضي مصلحة الدفاع عن البلاد أن تبقى سرا على غير من يناط بهم حفضها أو استعمالها. 3 - الأخبار والمعلومات المتعلقة بالقوات المسلحة وتشكيلاتها وتحركاتها وعتادها وتموينها وغير ذلك مما له مساس بالشؤون العسكرية والخطط الحربية ما لم يكن قد صدر أذن كتابي من جهة مختصة بنشره أو إذاعته. 4 - الاخبار والمعلومات المتعلقة بالتدابير والاجراءات التي تتخذ لكشف وضبط الفاعلين والشركاء في الجرائم المنصوص عليها في هذا الباب وكذلك الاخبار والمعلومات الخاصة بسير التحقيق والمحاكمة اذا حضرت سلطة التحقيق أو المحاكمة اذاعتها"، ومن أمثلة التجسس على إجراءات التحقيق هو قيام أحد الاشخاص في نيويورك، بالتنصت على محادثات النائب العام اثناء قيامه بالتحقيق، لمصلحة احدى الشركات التي استأجرته[1].

ومن الجدير بالذكر لا يعني السر اقتصاره على شخص واحد بل يمكن أن يكون بين عدة أشخاص، ولا ترتفع رغم ذلك صفة السرية[2]، كما يعتبر من حصل على أسرار الدفاع بوسيلة غير مشروعة متجسس حتى لو لم يقصد تسليم

(1) للمزيد: ياسر الامير فاروق محمد، مراقبة الاحاديث الخاصة في الاجراءات الجنائية، اطروحة دكتورا، جامعة القاهرة كلية الحقوق، 2008، ص 270 - 271.

(2) وجدي شفيق فرج، الجنايات والجنح المضرة بالحكومة من جهة الخارج والداخل، دار الكتب القانونية، القاهرة، 2010، ص 54.

الأسرار[1] أو إفشاءها[2]، كذلك لا يشترط التخفي[3] من أجل الحصول على السر، إذ قد يكون مفشي السر موظف أو مكلف بخدمة عامة اطلع على أسرار الدفاع بحكم عمله[4]، كما أن إفشاء السر لأكثر من مرة لا يمنع من العقاب على كل حالة إفشاء[5]، وعليه حتى تعتبر من أسرار الدفاع يجب تحقق شرطين، الأول أن تكون المعلومات ذات طبيعة سرية، والثاني أن تتعلق هذه الأسرار بالدفاع عن البلاد[6]، ومن الأمثلة على التجسس العسكري، تمكن قوات التحالف من إختراق أجهزة الاتصال العراقية و تعطيلها، مما أدى إلى قطع الاتصالات كلياً أو تغييرها بين قيادات الدولة و الجيش العراقي[7].

---

(1) تقسم الاسرار الى نوعين: اسرار طبيعية ويقصد بها (هي المعلومات أو الوثائق التي تعد بطبيعتها من الاسرار ولا يعلمها الا الاشخاص المنوط بهم حفظها وصيانتها لأن مصلحة الدفاع تقتضي ان تبقى سرا على من عداهم)، واسرار حكمية ويقصد بها(هي المعلومات أو الوثائق التي لا تتصف بالسرية بطبيعتها، وأنما وصفت بالسرية لأن اذاعتها و افشاءها يؤدي الى الوصول لسر حقيقي أو أنها بحكم الاسرار بمقتضى أمر السلطة المختصة).ينظر: د.أيمن عبد الحفيظ عبد الحميد سليمان، مرجع سابق، ص 160 - 161.

(2) للمزيد: المادة (80 / أ) من قانون العقوبات المصري.

(3) علي بن نايف الشحود، الخلاصة في احكام التجسس، ط 1، بدون دار نشر، بدون مدينة، 2011، ص 14.

(4) في هذا المعنى: وجدي شفيق فرج، مرجع سابق، ص 58. للمزيد: (الفقرة ب من المادة 80) من قانون العقوبات المصري.

(5) أسامة بن عمر محمد عسيلان، الحماية الجنائية لسر المهنة في الشريعة الاسلامية والقوانين الوضعية وتطبيقاتها في بعض الدول العربية، رسالة ماجستير، جامعة نايف العربية للعلوم الامنية - كلية الدراسات العليا، الرياض، 2004، ص 116.

(6) د. حسني فتحي مصطفى بهلول، عقد انتاج المعلومات والامتداد بها، دار الفكر الجامعي، الاسكندرية، 2008، ص 239.

(7) د. حسن بن احمد الشهري، الانظمة الإلكترونية الرقمية المطورة لحفظ وحماية سرية المعلومات من التجسس، المجلة العربية للدراسات الامنية والتدريب، جامعة نايف العربية للدراسات الامنية والتدريب، المجلد 28، العدد 56، 2012، ص 14.

ثانيا: المعلومات السياسية:

ويقصد بها (هي تلك المعلومات الخاصة بالسياسة الداخلية والخارجية للدولة، وكذلك المعلومات المتعلقة بالسفارات ونشاط عملها، والتي تشمل سياسة الدولة وخططها الاقتصادية والصناعية المتعلقة بمصلحة الدفاع، والتي يجب أن تبقى سرية إلا للمسؤول عن حفظ هذه الاسرار)[1]، وأسرار الدولة متعددة ومنها موقفها من بعض الأحداث التي تحصل بالدول المجاورة، أو رغبتها في قطع علاقاتها الدبلوماسية مع إحدى الدول....الخ[2].

ونجد من المناسب هنا تحديد مفهوم أسرار و وثائق الدولة السياسية منها وغير السياسية والبيانات الحكومية، كما حددتها بعض التشريعات، فقد أوضحت المادة (2) من قانون حماية أسرار ووثائق الدولة رقم (50) لسنة 1971 الأردني المقصود بأسرار ووثائق الدولة بالقول (هي أية معلومات شفوية أو وثيقة مكتوبة أو مطبوعة أو مختزلة أو مطبوعة أو ورق مشمع..... أو مايشابهها والمصنفة وفق أحكام هذا القانون)، كما تعرف البيانات الحكومية بأنها(تشمل بيانات الحكومة الاتحادية والحكومات المحلية والهيئات العامة والمؤسسات العامة الاتحادية والمحلية)[3].

وفي إطار التجسس السياسي نجد أن للبعثات الدبلوماسية الدور الكبير في جمع المعلومات السياسية ونقلها بواسطة حقائبهم التي كانت ولا تزال طريقة آمنة لنقل المعلومات والوثائق السرية وذلك لعدم خضوعها للتفتيش، يدعمها في ذلك أجهزة الاستخبارات، من خلال عملاء سريين يقومون بالتجسس وبالتالي

(1) د. حسن فتحي مصطفى بهلول، مرجع سابق، ص 240.
(2) للمزيد: وليد بن سعد محمد، مرجع سابق، ص 38.
(3) المادة (1) من القانون الاتحادي لمكافحة جرائم تقنية المعلومات الاماراتي.

رفدها بالمعلومات، والتي من أهمها المعلومات الماسة بأمن الدولة الخارجي[1]، كما يهدف التجسس السياسي إلى معرفة الأحزاب السياسية والقوى صاحبة النفوذ وأتجاهاتها، ومعرفة مواطن الضعف والقوى بين أبناء البلد ومدى ثقتهم بقياداتهم، ومعرفة الطوائف الدينية والقوميات وعلاقاتها ببعضها[2]. ويتفرع من الجاسوسية السياسية، الجاسوسية الاجتماعية التي تعنى بدراسة المقومات النفسية والمادية والتقاليد والعادات للشعوب[3].

(1) د. حسين المحمدي بوادي، الجاسوسية "لغة الخيانة"، دار الفكر الجامعي الاسكندرية، 2007، ص 44. د. محمد عودة الجبور، الجرائم الواقعة...، مرجع سابق، ص 203.

(2) د. سعد أبراهيم الاعظمي، جرائم التجسس...، مرجع سابق، ص 24.

(3) د. حسين المحمدي بوادي، مرجع سابق، ص 25 وما بعدها.

الفرع الثاني

المعلومات الاقتصادية و الصناعية و العلمية

اولا: المعلومات الاقتصادية:

ويقصد بها (الحقائق والوقائع والأخبار التي تتعلق بالانتاج الوطني الذي يسهم في زيادة مقاومة الدولة وصمودها في مواجهة العدوان أو التهديد به، أو هي كل ما يتعلق بالجهود الاقتصادية للبلاد والتي تمس الدفاع عنها ومن شأن افشائها إلحاق الضرر بالدولة [1]، وكل ما يتعلق بالبيانات الخاصة بالسياسات المالية والمخزون الاستراتيجي والحالة النقدية).

أما عن أساليب التجسس نجد هنالك أساليب خاصة للتجسس الاقتصادي، والذي يمارس من قبل شركات متخصصة بهذا الشأن، مثل جمعية محترفي التنافس المخابراتي التي تأسست في أمريكا عام 1982، ومن الأساليب المتبعة هو القيام بدور المتدرب في الشركات المنافسة من أجل التجسس عليها، أو استخدام أجهزة التنصت، أو سرقة الدفاتر والمستندات للشركات المنافسة...الخ[2] مستهدفين نوعية وحجم الخدمات التي تقدمها الشركة.

(1) وليد بن سعد محمد عوشن، مرجع سابق، ص 40.

(2) للمزيد: د. رواء زكي يونس الطويل، التجارة الالكترونية والتجسس الاقتصادي، مجلة آداب الرافدين، جامعة الموصل كلية العلوم السياسية، العدد 51، 2008.

وسنتناول في المعلومات الاقتصادية مايأتي.

1. **التجارة الالكترونية:**

عرفتها منظمة التجارة العالمية بأنها (عبارة عن عملية إنتاج وترويج وبيع وتوزيع المنتجات من خلال شبكة اتصال) [1]، وتواجه التجارة الالكترونية العديد من التحديات، من أهمها ضعف الأمن المعلوماتي وضعف حماية الخصوصية، فعلى مستوى البنوك العالمية لازالت لاتفضل الاعتماد في معاملاتها على البريد الالكتروني المرسل من المصارف الاخرى، إذ تفضل الابقاء على قنوات الاتصال التقليدية[2]، وهذا التخوف له مايبرره إذ يستطيع التجار من خلال استخدام بعض البرامج مثل برنامج (الكوكيز) والذي يقوم بالتقاط البيانات الشخصية واستغلالها لإغراق المستخدمين بالدعاية لمنتجاتهم[3]. و أن الحفاظ على هذه المعلومات يساهم في ازدهار التجارة الالكترونية، سواء تعلقت بالمستهلك أو البائع أو وسائل الدفع الالكترونية...الخ[4].

2. **التوقيع الالكتروني[5]:**

يعتبر التوقيع الالكتروني سببا في ازدهار التجارة الالكترونية[6]، وبالتالي يكون هدفاً للاعتداء بانتهاك سريته حالة في ذلك حال التجارة الالكترونية، وذلك بالاختراق من قبل الجاني بالدخول إلى النظام المعلوماتي أو اعتراضه، ويرى الفقه

(1) د. خالد ممدوح ابراهيم لوجستيات التجارة الالكترونية، ط 1، دار الفكر الجامعي، الاسكندرية، 2008، ص 130.

(2) د. عبد الفتاح بيومي حجازي، مقدمة في التجارة الالكترونية العربية (شرح قانون المبادلات والتجارة الالكترونية التونسي، ج1، دار الفكر الجامعي، الاسكندرية، 2003، ص 50 - 51.

(3) للمزيد: د. أيمن عبد الله فكري، جرائم نظم المعلومات /دراسة مقارنة، دار الجامعة الجديدة، الاسكندرية، 2007، ص 657 وما بعدها.

(4) د. عبد الفتاح بيومي حجازي، التجارة الالكترونية وحمايتها القانونية، مرجع سابق، ص 274.

(5) تعريف التوقيع الالكتروني ينظر ص (48) من الرسالة.

(6) في هذا المعنى: د. عبد الفتاح بيومي حجازي، التوقيع الالكتروني في النظم القانونية المقارنة، دار الفكر الجامعي، الاسكندرية، 2005، ص 186.

الجنائي الفرنسي أن عملية الاختراق أو الدخول إلى النظام المعلوماتي لها مدلول معنوي، كما لها مدلول مادي متمثل بدخول الشخص أو محاولة الدخول إلى النظام المعلوماتي، باستخدام برنامج أو شفرة خاصة أو كلمة السر الحقيقية أو أي وسيلة آخرى(1).

3.الحسابات المصرفية:

وتعرف السرية المصرفية بأنها(كتمان المصرف أسرار عملائه والاحتفاظ لنفسه بالمعلومات المتعلقة بأمورهم المالية، ومنع موظفيه من نقل المعلومات الخاصة بعميل إلى سواه من العملاء، أو إلى غير العملاء)(2)، حيث تلتزم المؤسسات المالية باتخاذ الاجراءات الكفيلة للحفاظ على سرية المعاملات المصرفية(3)، ومن صور الانتهاك للحسابات المصرفية، قيام القراصنة بالدخول غير المشروع إلى الحسابات المصرفية والسحب منها، أو يقومون بتحويل الاموال منها، وكذلك الاطلاع على حسابات العملاء، منتهكين بذلك السرية المصرفية(4)، وقد يتم الاطلاع على بيانات الذمة المالية وانتهاك سريتها بالالتقاط الهوائي لهذه البيانات المعالجة أو المنقولة ألكترونيا(5)، حيث استطاع بعض القراصنة من الحصول على تفاصيل بطاقات الائتمان، ومن ثم الدخول إلى انظمة التحويل المالي الخاصة بهذه البطاقات(6)،

(1) د.عبد الفتاح بيومي حجازي، اثبات المعاملات الالكترونية عبر الانترنت، دار النهضة العربية، القاهرة، 2009، ص 556 - 557.

(2) د. كمال طلبة المتولي سلامة، دور الدولة في حماية السرية والاستثناءات الواردة عليها مع عرض لأهم الاعلانات والمؤتمرات والدولية وموقف بعض الدساتير والقانون المقارن منها، ط 1، مركز الدراسات العربية، الجيزة، 2015، ص 90.

(3) المادة (25) من قانون التوقيع الالكتروني والمعاملات الالكترونية العراقي رقم 78 لعام 2012.

(4) حازم نعيم الصمادي، مرجع سابق، ص 53.

(5) د. طارق ابراهيم الدسوقي، مرجع سابق، ص 571.

(6) عبد الصبور عبد القوي علي المصري، التنظيم القانوني للتجارة الالكترونية، مكتبة القانون والاقتصاد، الرياض، 2012، ص 125.

أو يحصل الانتهاك من الموظفين في المصرف ذاته عند قيامهم بإفشاء أسرار عملاء المصرف سواء كانت شفاهة أم كتابة أم صراحة أم ضمنا، وتقوم مسؤولية هؤلاء الموظفون عما يفشونه حتى في حال انقضاء الوظيفة لأي سبب كالاستقالة وغيرها[1].

إلا أنه ترد استثناءات على السرية المصرفية، والتي يترتب عليها الافصاح عن البيانات المتعلقة بالعميل، ومنها الكشف عن السرية المصرفيه بناءً على طلب الجهات الرقابية، أو أمر صادر من السلطة القضائية، أو بناءً على موافقة العميل[2].

4. بطاقات الإئتمان:

تعرف بأنها: (أداة تمكن صاحبها من الإئتمان والدفع في ذات الوقت، فهي أداة دفع إذ تمكن العميل من دفع قيمة المشتريات مباشرةً، وهي أداة إئتمان إذ يستطيع العميل الحصول على الخدمات والسلع ويقوم المصرف بالسداد بدلاً عنه)[3]، أما عن الانتهاكات فقد تتعرض بطاقات الإئتمان للإعتداء وذلك بالالتقاط غير المشروع أو التجسس أو التنصت على البيانات الخاصة بالبطاقة الإئتمانية، والمعلومات الخاصة بالشركات التجارية الكبرى، باستخدام بعض التقنيات عبر شبكة الانترنت أو باستخدام كلمة السر[4]، مستهدفين بذلك الرقم أو

(1) د. محمد عبد اللطيف فرج، الحماية الجنائية للإئتمان المصري (دراسة تحليلية تأصيلية مقارنة)، دار النهضة العربية، القاهرة، 2006، ص 101 - 102.

(2) د. احمد السيد لبيب ابراهيم، الدفع بالنقود الالكترونية الماهيه والتنظيم القانوني دراسة تحليلية مقارنة، دار الجامعة الجديدة للنشر، الاسكندرية، 2009، ص 248 وما بعدها. د. محمد عبد اللطيف فرج، مرجع سابق، ص 164.

(3) د. عبد الرسول عبد الرضا و محمد جعفر هادي، المفهوم القانوني للتوقيع الالكتروني، مجلة المحقق الحلي للعلوم القانونية والسياسية، كلية القانون - جامعة بابل، العدد 1، السنة الرابعة، ص 177.

(4) د. مصطفى محمد موسى، التحري في جرائم مجتمع المعلومات والمجتمع الافتراضي، دار النهضة العربية، القاهرة، 2011، ص 525. د. أيهاب فوزي السقا، مرجع سابق، ص 204.

الاسم الموجود على بطاقة الائتمان أو تاريخ الاستحقاق، واستخدام هذه المعلومات لحساب المتجسس أو بيعها للشركات المنافسة[1]، وقد أولى المشرع الفرنسي بطاقة الائتمان حماية خاصة بالمادة (11) من قانون رقم 1383 لسنة[2] 1991.

ومثال على اختراق بطاقات الإئتمان ما قام به حدث امريكي يبلغ من العمر اثني عشر سنة يدعى (جستين بترس)، حيث تمكن من اختراق شبكة وكالة TRW لخدمة بطاقات الائتمان، وسرقة بيانات مجموعة من بطاقات الإئتمان من جهاز الحاسب الخاص بالوكالة[3].

ثانيا: المعلومات الصناعية:

تعرف بأنها: (الحقائق المتعلقة بسر صناعة معينة تنتجها المصانع وتعول عليها الدول في التعبئة الاقتصادية، سواء ادرجتها الدولة صراحة في خطة الدفاع الوطني، أو كان من شأنها أن تخدم هذة الخطة، ولايقتصر الأمر على الانتاج الصناعي للدولة، بل تمتد إلى الشركات الخاصة التي تستفييد الدولة من انتاجها في الدفاع عن البلاد)[4]، حيث يعزز الحفاظ على السر الصناعي مثلا حماية الصناعات الوطنية من المنافسة غير المشروعة[5]، فقد تعرضت أهم المعلومات على مستوى العالم للإختراق من قبل مراهقين في ولاية كاليفورنيا إذ تمكنوا من اختراق موقع شبكة المعلومات لمختبر (سانديا) ومختبر(أوك ريدج) الامريكيين الخاصان ببرنامج الأسلحة النووية[6]، كما تمكن الجواسيس السوفيت من الحصول على

(1) نضال اسماعيل برهم، أحكام عقود التجارة الالكترونية، ط 1، دار الثقافة، عمان، 2004 ص 127 - 128.

(2) د. حسين بن سعيد الغافري، مرجع سابق، ص 292 ومابعدها.

(3) د. عبد الفتاح بيومي حجازي، الاحداث والانترنت، دار الفكر الجامعي، الاسكندرية، 2004، ص 210.

(4) أسامة بن عمر محمد عسيلان، مرجع سابق، ص128-129. وليد بن سعد محمد عوشن، مرجع سابق، ص41.

(5) د. هشام ليوسفي، الحماية الجنائية للسر المهني، ط1، دار الوليد، القاهرة، 2015، ص 61.

(6) د. عبد الفتاح بيومي حجازي، الاحداث والانترنت، مرجع نفسه، ص 229 - 230.

اسرار القنبلة الذرية، التي يقدر الخبراء ثمن الحصول عيها بملايين الدولارات، اضافة الى اختصار الجهد في التجارب الباهضة التكاليف[1].

ثالثا: المعلومات العلمية:

ويقصد بها (المعلومات المتعلقة بالابحاث والدراسات والاختراعات العلمية على مختلف الاصعدة العسكرية والصناعية وغيرها، ويهتم التجسس العلمي بالاطلاع على هذه الاسرار العلمية بهدف سرقتها أو بهدف اتخاذ الاحتياطات اللازمة لمواجهتها) [2]، وعليه فإن التجسس العلمي يرتكز على الوصول للمعلومات التي وصلت إليها الدول في مجال التقدم العلمي كالتطور ببرامج الفضاء أو في صناعة الاسلحة وغيرها، و أن معيار نجاح المتجسس هنا أن تكون المعلومات العلمية التي تم الحصول عليها قد تمت دون معرفة الدولة المتجسس عليها[3]. كما وتتعرض المعلومات الطبية المسجلة في النظام المعلوماتي للإنتهاك من قبل المسؤول عن النظام الالكتروني، إذ يقوم بإفشاء هذه البيانات والتي تستخدم في الابحاث العلمية، إلى جهات تجري أبحاثا بخصوص أمراض معينة [4].

(1) د. حسين المحمدي بوادي، الجاسوسية...، مرجع سابق، ص 18.
(2) د. علي جعفر، مرجع سابق، ص 570 - 571.
(3) د. حسين المحمدي بوادي، الجاسوسية...، مرجع سابق، ص 29، 30.
(4) د. عبد الفتاح بيومي حجازي، التجارة الالكترونية العربية، مرجع سابق، ص 282.

الفرع الثالث

المعلومات المتعلقة بالحياة الخاصة

أولا: تعريف الحياة الخاصة:

هي (ما يقوم به الشخص ولا يقبل أن يطلع عليه الغير، احتراما لسريته وخصوصيته من أي تدخل مادي أو معنوي)[1].

وتعرف أيضا بأنها(حق الشخص بالاحتفاظ بأسرار من الصعب على العامة معرفتها إلا بإرادته، والتي تتعلق بحقوقة الشخصية، وأن الحق في الحياة الخاصة تقع في دائرة الحقوق الشخصية وأن كان لا يشملها كلها)[2].

حيث يقرر القانون حماية سرية وحرمة المراسلات والمخابرات الهاتفية، ويمنع إفشاءها حتى على من اطلع عليها بحكم وظيفته، والتي لا يجوز إفشاء سريتها إلا في الحالات المقررة قانونا[3].

ومن الجدير بالذكر أن المعلومات المجهولة التي لاتدل على صاحبها، لاتثير أي مشكلة لأن المجهول لا خصوصية له، ولكن المشكلة تثور عند دلالة هذه المعلومات على أشخاص معروفين[4]، وللاعتداء على الحياة الخاصة صور عديدة منها.

(1) أنسام سمير طاهر الحجامي، الحماية الجنائية لتكنلوجيا المعلومات، رسالة ماجستير، جامعة كربلاء – كلية القانون، 2013، ص 73. عبد الصبور عبد القوي علي مصري، مرجع سابق، ص 303.

(2) د. فتوح الشاذلي و عفيفي كامل عفيفي، جرائم الكومبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون /دراسة مقارنة، ط2، منشورات الحلبي الحقوقية، بيروت 2007، ص 308.

(3) د. محمد حسين منصور، مرجع سابق، ص 264.

(4) د. بولين انطونيوس ايوب، الحماية القانونية للحياة الخاصة في مجال المعلومات، ط 1، منشورات الحلبي الحقوقية، بيروت، 2009، ص 104.

فبالنسبة لفض الرسائل، حيث يطلع الشخص على مضمون ومحتوى رسالة أو برقية ارسلت إلى الغير، ولا يشترط لتوفير الحماية للرسائل أن تحوي على أسرار، متعلقة بشخص المرسل أو المرسل إليه[1]، هذا هو الأصل العام لكن الامر مختلف إذا كانت هنالك حاجة لذلك.

كما ذهبت إلى ذلك محكمة النقض المصرية في قرارها الصادر عام 1962 حيث جاء فيه (الأصل أنه لايجوز إفشاء الأسرار والتلغراف والاطلاع عليها ومراقبة المكالمات التلفونية غير أنه إذا استلزمت مصلحة التحقيق ذلك، فإنها تكون مصلحة أولى بالرعاية من الحفاظ على أسرار هذه المكاتبات والمكالمات)[2].

أما عن اختراق البريد الالكتروني فهو محل للاختراق من قبل الغير، وبالتالي فضح أسرار صاحب الشأن والحاق الضرر الجسيم به، فعلى سبيل المثال تمكن احد المخترقين من الدخول الى البريد الالكتروني للمشتركين لدى (Hotmail) واذاعة اسرار المشتركين فيه، وكانت شركت مايكروسوفت مالكة للموقع[3]، وقد يكون البريد الالكتروني هدفاً للتجسس من الحكومات[4]، أوقيام المخترقين بتحريف الصور الشخصية للنساء، وذلك بوضعها على صورة لإمرأة عارية وارسالها الى عدد من الاشخاص من خلال البريد الالكتروني[5]، وقد اصدرت محكمة القضاء المستعجل في فرنسا في قضية في هذا الخصوص تتلخص

(1) شمسان ناجي صالح الخيلي، الجرائم المستخدمة بطرق غير مشروعة لشبكة الانترنت، القاهرة، 2009، ص98.

(2) أشار اليه: د. طارق صديق رشيدكه ردى، حماية الحرية الشخصية في القانون الجنائي (دراسة تحليلية مقارنة)، ط1، منشورات الحلبي الحقوقية، بيروت، 2011، ص 232.

(3) أسعد فاضل منديل، البريد الالكتروني دراسة قانونية، مجلة القانون المقارن، الكلية الاسلامية الجامعة - محافظة القادسية، العدد 57، 2008، ص140.

(4) للمزيد: د. بولين انطونيوس ايوب، مرجع سابق، ص 102.

(5) عدي جابر هادي، الحماية الجزائية للبريد الالكتروني، مجلة رسالة الحقوق، العدد 3، جامعة القادسية كلية القانون، 2010، ص 161.

بقيام شخص بتحريف صور لطالبة تظهرها عارية وبثها على الانترنت، بأن أصدرت أمر الى متعهد الوصول باستخدام الوسائل التقنية التي من شأنها منع بث الصور العارية على الانترنت التي تمت دون موافقتها، وفرضت غرامة تهديدية مقدارها (مئة الف فرنك) عن كل يوم تأخير، كما الزمت المحكمة متعهد الايواء بضرورة احترام قواعد الاخلاق والاداب العامة لمن يقوم بتزويدهم بالمعلومات، واحترام قواعد وآداب المهنة التي تحكم شبكة الانترنت[1].

ومن الجدير بالذكر هو وجود فراغ تشريعي في القوانين العراقية فيما يخص الجرائم المعلوماتية، حيث قام أحد الاشخاص باختراق البريد الإلكتروني الخاص بشريكه في الشركة ومعرفة رقمه السري، وقد أقام المجني عليه دعوى ضد شريكه أمام محكمة جنح المسيب، إلا أن المحكمة قررت الغاء التهمة الموجهة الى المتهم، وذلك لعدم وجود نص نافذ يجرم الفعل ولا يجوز القياس في الامور الجنائية استنادا الى مبدأ (لا جريمة ولا عقوبة الا بنص)، وقد صادقت محكمة استئناف بابل قرار محكمة جنح المسيب [2].

كما وتتعرض المعلومات الشخصية للانتهاك أيضا من خلال جمع معلومات حقيقية بدون ترخيص[3]، يكون ذلك بالتقاط الارتجاجات التي تحدثها الاصوات في الجدران الاسمنتية، والقيام بعد ذلك بمعالجتها بواسطة حاسب مزود ببرنامج خاص لترجمتها الى كلمات، أو عن طريق اعتراض الرسائل المتبادلة بالبريد الالكتروني، و توصيل اسلاك بطريقة خفية إلى الحاسب الذي يحتوي البيانات، أو

(1) د. حسين بن سعيد الغافري، مرجع سابق، ص 624.

(2) قرار محكمة استئناف بابل الأتحادية ذي العدد(120/جزائية/2011) في تاريخ(2011/4/28) قرار غير منشور. أشار إليه: أنسام سمير طاهر الحجامي، مرجع سابق، ص 90.

(3) Prof. Dr. Marco Gercke. Understanding cybercrime Phenomen, report. Presented toITU Telecommunication Development Bureau. Entitled challenges and legal response 2012. Page 2.

التنصت على المكالمات أو التسجيل دون الحصول على إذن من القضاء[1]، أو يكون جمع تلك المعلومات الشخصية بترخيص لكن يقوم المسؤول عن حفظها بأفشائها[2].

أما بالنسبة الى التقاط صور للغير دون رضاهم، فتكون بقيام البعض بإلتقاط صور للسيدات في الطرق العامة دون رضاهن، بواسطة الهواتف المحمولة، مما دفع بعض الدول لأتخاذ خطوات صارمة، ومنها مثلا ما قامت به المملكة العربية السعودية، بأن عاقبت من يعتدي على الحياة الخاصة بواسطة أجهزة الهاتف التي تحوي كامرات[3]، و جَرَّمَتْ بيع أجهزة الهاتف التي تحتوي آلة تصوير[4]، ويمتد العقاب إلى الموظف الذي يقوم بالتقاط صور للغير دون رضاهم مستغلا بذلك وظيفته[5]، ولا فرق إن كانت الصورة التي التقطت ظلت على حالتها أو ان الفاعل قد ادخل عليها بعض التغييرات[6]، وقد أقامت أحدى الممثلات دعوى أمام محكمة نيورك تطلب فيها إلزام المدعى عليه، وهو أحد المصورين بمنع نشر صورة التقطت لها في إحدى المسارح وهي ترتدي ملابس فاضحة، وقد صدر حكم من المحكمة بمنع نشر تلك الصورة، مسببةً حكمها بأن نشرها يمثل إعتداء على الخصوصية[7]، وعليه يشترط لتحقق الاعتداء أن تكون الصورة قد التقطت لشخص وليس لوثيقة أو شئ أو غير ذلك، وأن يتم الالتقاط بأي جهاز مخصص لذلك فلا تقوم الجريمة إذ ما قام شخص برسم صورة لشخص آخر، كما يجب أن تكون قد التقطت دون

(1) د. فتوح الشاذلي و عفيفي كامل عفيفي، مرجع سابق، ص 276.

(2) أنسام سمير طاهر الحجامي، مرجع سابق، ص 83.

(3) عبد الصبور عبد القوي علي مصري، مرجع سابق، ص 121.

(4) منى فتحي احمد عبد الكريم، مرجع سابق، ص 45.

(5) محمد احمد ابو زيد احمد، موسوعة القضاء الجنائي، المركز القومي للأصدارات القانونية، القاهرة، 2008، ص 516 - 517.

(6) عبد الحكيم ذنون يونس يوسف الغزال، الحماية الجنائية للحريات الفردية "دراسة مقارنة"، أطروحة دكتورا، جامعة الموصل - كلية القانون، 2003، ص 206.

(7) أشار اليه: د. محمد الشهاوي، مرجع سابق، ص 243.

رضا المجني عليه، كما يشترط أن تكون الصورة قد التقطت في مكان خاص بالمجني عليه[1] أو في مكان عام ولكن فيها إعتداء على الخصوصية كما ذهبت الى ذلك محكمة نيورك في المثال السابق.

أما عن التنصت على المحادثات والحديث الخاص[2]، فقد استقر الفقه على اعتبار أن الاعتداء على الحياة الخاصة موجود في حال صدور المحادثات أو الحديث في مكان خاص، اي بصورة مباشرة أو بصورة غير مباشرة[3] عن طريق الهاتف أو أي جهاز آخر باستراق السمع أو التسجيل[4] أو النقل[5] للمكالمات الهاتفية الخاصة[6]، باستخدام مثلا برنامج (FlexiSPY) والذي يثبت على الهواتف اللوحية المتطورة لغرض التجسس على المكالمات والرسائل القصيرة[7]، كما استطاعت المانيا بالاضافة الى اصطياد الاشارة من الهواتف وتحويلها الى كلمات مسموعة، من معرفة اماكن المتحدثين[8]. ومن صور الاعتداء قيام احد الاشخاص بوضع جهاز تسجيل دقيق خارج مسكن الضحية، يقوم بتسجيل مايدور

(1) د. محمد الشهاوى، مرجع نفسة، ص 318 ومابعدها.

(2) الحديث الخاص يقصد به: (صوت له دلالة مفهومة سواء على نطاق واسع لجمهور الناس أم لفئة معينة منهم ولا عبرة باللغة التي يتحدث بها فان انتفى وصف الحديث عن الصوت فان الجريمة لا تقوم كاصوات الالحان الموسيقية أو الصيحات التي ليس لها دلالة معينة). ينظر: عبد الحكيم ذنون يونس يوسف الغزال، مرجع سابق، ص 204.

(3) جمال عبد الناصر عجالي، الحماية الجنائية من اشكال المساس بحرمة الحياة الخاصة عبر المكالمات والصور، رسالة ماجستير، جامعة محمد خضيرة كلية الحقوق والعلوم السياسية، 2014، ص 82.

(4) تسجيل الحديث يقصد به: (حفظ الحديث على الشريط المخصص لذلك ويتم الاستماع اليه بعد ذلك). ينظر: د. محمد الشهاوي، مرجع سابق، ص 265.

(5) نقل الحديث يقصد به: (أستراق السمع بواسطة جهاز لأرساله من المكان الذي أجرى فيه الحديث الى مكان آخر بأستخدام جهاز محدد). ينظر: د. محمد الشهاوي، مرجع سابق، ص 265 - 266.

(6) منى فتحي أحمد عبد الكريم، مرجع سابق، ص 47.

(7) د. حسن بن احمد الشهري، مرجع سابق، ص 12.

(8) محمد خليل الحكايمة، مرجع سابق، ص 39.

من كلام داخله، حيث جرمت المحكمة العليا في امريكا مثل هكذا تصرف في قضية شهيرة باسم (كلينتون ضد فرجينيا) في عام 1964، وقد ظهر اتجاهين في تحديد الحديث الخاص، احدهما يعتمد على (موضوع الحديث) في تحديد الحديث الخاص والذي تبنته امريكا وايضا فرنسا بموجب(الفقرة 1 من المادة 226) من قانون العقوبات الفرنسي الجديد، حيث جرمت كل اعتداء بالتنصت او التسجيل او النقل على ألفة الحياة الخاصة، دون رضا الشخص نفسه[1]، أما الاتجاه الآخر فإنه يعتمد (مكان الحديث) وذلك بتجريم قيام الشخص الذي له حق الدخول الى مكان بأذن من صاحب المكان، يقوم بوضع جهاز تسجيل، وهنا يعتبر بمثابة ادخال شخص ثالث الى المكان، إلا وهو جهاز التسجيل الذي يعتبر منتهك لمبدأ الحرية الشخصية[2].

ومن الجدير بالذكر نجد هنالك حكم للمحكمة العليا في أمريكا تعتبر فيه التنصت على المتهم لايعتبر خلسة عنه[3]، يعتقد البحث أن في الحكم المتقدم انتهكت المحكمة النصوص الدستورية والقانونية في أمريكا التي تأكد على حرمة الحياة الخاصة والتي لا يجوز انتهاكها الا وفقاً للقانون.

(1) ياسر الامير فاروق محمد، مرجع سابق، ص 528 - 529.

(2) د. توفيق محمد الشاوي، حرمة اسرار الحياة الخاصة ونظرية عامة للتفتيش، منشأة المعارف، الاسكندرية، 2006، ص 236. د. طارق صديق رشيدكه ردى، مرجع سابق، ص 220.

(3) نزيه نعيم شلال، مرجع سابق، ص 17.

الفصل الثالث

بعض صور جريمة التجسس المعلوماتي

للتجسس المعلوماتي عدة صور من أهمها الدخول غير المشروع، الذي اتسع مفهومه ليشمل بعض صور السلوك المادي للجرائم الاخرى كالاعتراض أو الالتقاط أو التنصت المعلوماتي كما سنبين ذلك، وتستخدم في ارتكابها تقنية المعلومات والاقمار الصناعية وطائرات التجسس...الخ، وعزز ذلك استخدام شبكة الانترنت في تأمين الاتصالات و تبادل المعلومات أو البيانات، مما جعلها تشكل تهديدا حقيقيا لأمن الدول والمؤسسات التجارية والصناعية وللحياة الخاصة...الخ، فشرعت القوانين التي تجرم هذه الصور.

وتأسيسا على ما تقدم، سنتناول في هذا الفصل صور جريمة التجسس المعلوماتي، و ذلك من خلال مبحثين:

- نستعرض جريمة الدخول غير المشروع في **المبحث الاول**.
- ونبين جريمة الاعتراض أو الالتقاط أو التنصت المعلوماتي **في المبحث الثاني**، وعلى النحو الآتي.

المبحث الاول

جريمة الدخول غير المشروع

سنبين في هذا المبحث، أركان هذه الجريمة وعقوباتها وذلك في مطلبين، يخصص المطلب الاول لأركان جريمة الدخول غير المشروع، ونفرد المطلب الثاني للعقوبة.

وقبل استعراض أركان الجريمة والعقوبة لا بد من إيراد النصوص القانونية التي جرمة الدخول غير المشروع.

فبالنسبة للتشريع الفرنسي فقد جرمها في (الفقرة 1 من المادة 323) من قانون العقوبات الفرنسي الجديد حيث نصت على أن " الدخول أو البقاء بطريق الغش داخل كل أو جزء من نظام المعالجة الآلية للمعطيات، يعاقب عليه بالحبس لمدة سنة وغرامة مقدارها(100، 000) فرانك، فإذا نجم عن هذا الدخول محو أو تعديل في المعطيات المخزونة في النظام أو إتلاف تشغيل هذا النظام تكون العقوبة الحبس لمدة سنتين وغرامة مقدارها (200، 000) فرانك ".

أما التشريع الامريكي فقد جرم الدخول أو البقاء غير المشروع ولكن مستخدما عبارة الدخول العمدي بدون تصريح أو تجاوز التصريح، كما استخدمت عبارة الوصول عمدا بدون ترخيص أو تجاوز الترخيص.

إذ نصت (الفقرة أ من المادة 1030) من قانون إساءة استخدام الحاسب لعام 1984 المعدل على تجريم الدخول العمدي الى الحواسيب الحكومية أو المتعلقة بأعمال الحكومة حيث نصت على أن " 1 - الدخول العمدي إلى جهاز الحاسوب بدون تصريح أو تجاوز للتصريح الممنوح له، ويحصل بأيه وسيلة على معلومات تقررت من قبل حكومة الولايات المتحدة بناء على أمر تنفيذي وتصريح

برلماني يتطلب الحماية، ضد الافشاء غير المخول به لأسباب تتعلق بالدفاع الوطني أو العلاقات الأجنبية. 2 - الوصول عمدا الى الحاسوب بدون ترخيص، أو تجاوز الترخيص الممنوح بقصد الحصول على معلومات واردة في سجل مالي بمؤسسة مالية، أو أن تشمل هذه المعلومات المتضمنة في ملف وكالة أو معلومات من أي حاسب محمي إذا تعلق بمحتوى اتصالات خارجية أو بين الولايات. 3 - الوصول العمدي بدون ترخيص لأي حاسوب غير عام يخص إحدى إدارات أو وكالات الولايات المتحدة مخصص لاستعمال حكومة الولايات المتحدة، أو لم يكن مخصص لها ولكن استعمل من قبل أو لأجل حكومة الولايات المتحدة الأمريكية وكان ذلك التصرف مؤثرا على ذلك الاستعمال من قبل أو لأجل حكومة الولايات المتحدة ".

أما النظام السعودي لمكافحة جرائم المعلومات فقد نص على تجريم الدخول غير المشروع في (الفقرة 2 من المادة 7) " الدخول غير المشروع الى موقع الكتروني، أو نظام معلوماتي مباشرة، أو عن طريق الشبكة المعلوماتية، أو إحدى أجهزة الحاسب الآلي للحصول على بيانات تمس الامن الداخلي أو الخارجي للدولة أو اقتصادها الوطني".

أما التشريع الاماراتي فقد استخدم عبارة الدخول دون تصريح في نص المادة (4) من المرسوم بالقانون رقم (5) لعام 2012 لمكافحة جرائم تقنية المعلومات على أن" يعاقب بالسجن المؤقت والغرامة التي لا تقل عن مائتين وخمسون الف درهم ولا تتجاوز مليون وخمسمائة الف درهم، كل من دخل بدون تصريح الى موقع الكتروني، او نظام معلوماتي الكتروني، أوشبكة معلوماتية، أوسيلة تقنية معلومات، سواء كان الدخول بقصد الحصول على بيانات حكومية، أو معلومات سرية[1] خاصة بمنشأة مالية أو تجارية أو أقتصادية. وتكون العقوبة

(1) يقصد بالسرية " أي معلومات أو بيانات غير مصرح للغير الاطلاع عليها أو بأفشاءها الا بأذن مسبق ممن يملك هذا الاذن". ينظر: المادة (1) من مرسوم مكافحة جرائم تقنية المعلومات الاماراتي.

السجن مدة لا تقل عن خمسة سنوات والغرامة التي لا تقل عن خمسمائة الف درهم ولا تتجاوز مليونين درهم، إذا تعرضت هذه البيانات أو المعلومات للإلغاء أو الحذف أو الإتلاف أو التدمير أو الافشاء أو التغير أو النسخ أو النشر أو إعادة النشر".

أما مشروع قانون الجرائم المعلوماتية العراقي لعام 2012 فقد نص بالمادة (3) على تجريم الدخول أو البقاء غير المشروع حيث نصت على أن " أ - الدخول أو البقاء أو اتصال غير المشروع مع كل أو جزء من تقنية المعلومات أو الاستمرار به. ب - محو أو تعديل أو تشويه أو نسخ أو نقل أو تدمير للبيانات المحفوظة وللأجهزة والانظمة الالكترونية وشبكات الاتصال والحاق الضرر بالمشتركين والمستفيدين. ج - الحصول على معلومات حكومية سرية ".

المطلب الاول

أركان جريمة الدخول غير المشروع

سنتناول في هذا المطلب أركان جريمة الدخول غير المشروع المادي والمعنوي والركن المفترض (المحل) وعلى النحو الاتي.

- **الفرع الاول:** الركن المادي.
- **الفرع الثاني:** الركن المعنوي.
- **الفرع الثالث:** الركن المفترض (المحل).

الفرع الاول

الركن المادي

عرفت المادة (28) من قانون العقوبات العراقي الركن المادي للجريمة بأنه "سلوك إجرامي بارتكاب فعل جرمه القانون أو الامتناع عن فعل أمر به القانون "، و يمثل الركن المادي المظهر الخارجي الملموس، وله ثلاثة عناصر هي السلوك الاجرامي و النتيجة الجرمية والعلاقة السببية وهذا ماسنوضحه تباعا.

أولا: السلوك الاجرامي:

يعرف الدخول غير المشروع لغة: يأتي بمعنى تخلل[1] أو دخل المكان[2]، وتعني دخول البعض في البعض بمعنى الدخيل[3]، وكذلك دخول القانص في المكان الخفي ليختل قنصا[4].

أما غير المشروع: يقال شرع وشروعا وشرعا فهو شارع والجمع الشرع[5]، تعني ما شرع الله لعباده من الدين[6]، وتعني غير المشروع مجتمعه، أرتكاب أمر غير مشروع[7]، وتعني أيضا العمل الذي لا يستند الى تفويض قانوني[8].

(1) الصاحب بن عباد، مرجع سابق، ج2، ص 387.

(2) إسماعيل بن حماد الجوهري، تحقيق أحمد عبد الغفور عطار، ج 1، مرجع سابق، ص 114.

(3) محمد بن يعقوب الفيروز آبادي، تحقيق محمد نعيم العرقسوسي، القاموس المحيط، ج 3، ط 8، مؤسسة الرسالة، دمشق، 2005، ص 92.

(4) الخليل بن احمد بن عمرو، تحقيق مهدي المخزومي و أبراهيم السامرائي، معجم كتاب العين، ج 1، دار الحرية للطباعة، بيروت، 1985، ص 351.

(5) الخليل بن احمد بن عمرو، تحقيق مهدي المخزومي و أبراهيم السامرائي، ج1، مرجع نفسه، ص 58 - 59.

(6) إسماعيل بن حماد الجوهري، تحقيق أحمد عبد الغفور عطار، مرجع سابق، ج1، ص 353.

(7) أبراهيم مصطفى وأخرون، مرجع سابق، ج1، ص 656.

(8) حارث سليمان الفاروقي، المعجم القانوني عربي - أنكليزي، ج4، مكتبة لبنان، بيروت، 1972، ص 276.

قانونا : يعرف الدخول غير المشروع بأنه " دخول شخص بطريقة متعمدة الى حاسب آلي، أو موقع الكتروني، أو نظام معلوماتي أو شبكة حاسبات آلية غير مصرح لذلك الشخص بالدخول اليها[1] ".

فقها : يعرف الدخول غير المشروع بأنه (عملية إقتحام الأنظمة أو الشبكات الخاصة بأفراد أو منظمات خاصة أو حكومية، بمساعدة بعض البرامج المتخصصة في فك وسرقة كلمات السر وتصريحات الدخول بهدف الاطلاع على المعلومات أو تخريجها أو سرقتها)[2].

وأيضا (بأنه الولوج غير المصرح به أو بشكل غير مشروع الى نظام معالجة آلية للبيانات باستخدام الحاسوب، ويتحقق بالوصول الى المعلومات والبيانات المخزونة داخل النظام المعلوماتي دون رضا المسؤول عن هذا النظام أو المعلومات التي يحتوي عليها)[3].

وهنالك من عرفه بأنه (هو الوصول الى المعلومات و البيانات المخزونة داخل النظام المعلوماتي، دون موافقة صاحب هذة البيانات أو المعلومات، والذي يترتب عليه خسائر، والتي قد تترتب بمجرد محاولة وقف التدخل، ولو لم يترتب أضرار فعلية بالنظام أو بالبيانات التي يحويها النظام المعلوماتي)[4].

في حين يذهب الفقه الفرنسي الى أن الدخول غير المشروع له مدلولان مادي ومعنوي، يشبه المدلول المادي محاولة الشخص الدخول الى النظام المعلوماتي أو دخوله بالفعل، وللدخول والبقاء غير المشروعين صورة بسيطة تتمثل بالدخول أو البقاء في نظام معلوماتي ليس من حق الفاعل الدخول أو البقاء فيه، أما الصورة

(1) ينظر: (الفقرة 7 من المادة 1) من نظام مكافحة الجرائم المعلوماتية السعودي.
(2) منصور بن سعيد القحطاني، مرجع سابق، ص 34.
(3) د. أيمن عبد الله فكري، مرجع سابق، ص 221 - 222.
(4) د. احمد محمود مصطفى، مرجع سابق، ص 248.

المشددة تتمثل بتحقيق نتيجة جرمية على ذلك الدخول أو البقاء، أما المدلول المعنوي للدخول غير المشروع في النظام المعلوماتي يشبه الدخول الى ذاكرة الانسان، والذي يتحقق بأي صورة من صور التعدي المباشرة أو غير المباشرة[1]، والنتيجة في مجال بحثنا الحصول على بيانات سرية. وقد يكون الدخول من أشخاص غير مخولين يقومون بدخول النظام المعلوماتي بالاختراق وهم أشخاص من خارج المؤسسات يظهرون بمظهر شخص مصرح له بالدخول أو باستغلال نقاط الضعف بالنظام[2]، أو يتم الدخول من قبل الموظفين السابقين في المؤسسات مستخدمين كلمة السر الحقيقية الخاصة بالنظام المعلوماتي. ويتم الدخول غير المشروع بعدة طرق منها استخدام جهاز لفتح الشفرات أو تخمين كلمة السر للحاسب المستهدف، أو الدخول بعد تفجير الموقع المستهدف وذلك بإرسال عدد هائل من الرسائل وهذة الطريقة تستخدم لإستهداف الحواسيب المركزية للبنوك والمؤسسات المالية[3]، أو يدخل الفاعل باستخدام الحيله وذلك بإرسال رسالة من خلال شبكة الانترنت يطلب منك تحميل لعبة أو برنامج وهي بالحقيقة برامج تجسس، أو قيام الفاعل بوضع هذة البرامج التجسسية داخل البرامج الاصلية، والتي تقوم بتسجيل الشفرات التي يستخدمها اصحابها الشرعيون اثناء دخولهم إلى الحاسوب، وهذه الطريقة الأخيرة قد تم اتباعها للدخول الى الحواسيب الخاصة بوكالة الفضاء الامريكية (ناسة)[4]، كما يتحقق الدخول غير المشروع الى النظام المعلوماتي باخترق الفاعل القيود التي وضعها مالك النظام المعلوماتي، كأن يكون الفاعل مخول للدخول

(1) د.عبد الفتاح بيومي حجازي، مكافحة جرائم الكومبيتر....، مرجع سابق، ص 355 وما بعدها.

(2) د. عادل عزام سقف الحيط، مرجع سابق، ص 136.

(3) د. حسين بن سعيد الغافري، مرجع سابق، ص 277 وما بعدها. د. سليمان أحمد فضل، مرجع سابق، ص 172.

(4) د. عمر ابو الفتوح عبد العظيم الحمامي، مرجع سابق، ص 223. د. عبد الفتاح بيومي حجازي، الجرائم المستحدثة....، مرجع سابق، ص 79. د. نائلة عادل محمد فريد قورة، مرجع سابق، ص 315 وما بعدها. د. عماد مجدي عبد الملك، مرجع سابق، ص 118 - 119.

في جزء من النظام المعلوماتي فيتجاوز إلى جزءً آخر[1]، وبذلك يتحقق الدخول غير المشروع حتى من قبل الموظفين بالمؤسسات[2]، ويتحقق أيضا في كل استعمال للحاسب بدون رضا صاحبه، أيا كان نوع ذلك الاستعمال أو بإجراء أي اتصال بالنظام محل الحماية[3]، سواء بتمكن الفاعل من فتح النظام المعلوماتي مباشرة أو عن بعد وذلك باعتراض عمليات الاتصال للدخول الى النظام المعلوماتي[4].

ومن الجدير بالذكر أن خلافا فقهيا ثار حول مدى اعتبار مشاهدة (قراءة) البيانات دخولا غير مشروع، فهنالك من ذهب أن الدخول غير المشروع للنظام المعلوماتي يتحقق بمشاهدة البيانات على شاشة الحاسب، بحجة أن الدخول الى النظام المعلوماتي لا يتطلب أية وظيفة ينفذها الحاسب استجابة لنشاط الجاني[5].

في حين يرى آخر أن مجرد قراءة المعلومات الموجودة على الشاشة لا تعد دخولا غير مشروع الى النظام المعلوماتي، وكذلك الحال في الدخول الى برنامج منعزل عن النظام المعلوماتي[6]، ويضاف الى ذلك أن بعض الفقهاء يرى في أن التوسع في مفهوم النظم المعالجة آليا ترتب عليه اعتبار التقاط الاشارات الناجمة عن تبادل المعلومات والاطلاع عليها أو التنصت المجرد عليها دخولا غير مصرح به الى النظام المعلوماتي، والذي يتم باستخدام تقنية الاتصالات الحديثة، كالربط

(1) د. عبد الفتاح بيومي حجاز، الجرائم المستحدثة....، مرجع سابق، ص 484.

(2) د. نائلة عادل محمد فريد قورة، مرجع سابق، ص 336 وما بعدها.

(3) د. عبد الفتاح بيومي حجازي، الجرائم المستحدثة...، مرجع سابق، ص 483. د. أيمن عبد الله فكري، مرجع سابق، ص 222.

(4) سورية بنت محمد الشهري، مرجع سابق، ص 39. د. عبد الفتاح بيومي حجازي، الجرائم المستحدثة...، مرجع سابق، 524 - 525.

(5) د. نائلة عادل محمد فريد قورة، مرجع سابق، ص 341.

(6) د. عبد الفتاح بيومي حجازي، الجرائم المستحدثة...، مرجع سابق، ص 484. وكذلك: مؤلفه، التجارة الالكترونية وحمايتها القانونية، مرجع سابق، ص 336.

المباشر على خط الهاتف أو بتحويل المكالمات الهاتفية عن مسارها[1]. لكن لا أتفق مع الاراء المتقدمة على اعتبار أن ما ذكر من سلوك إجرامي هو سلوك إجرامي لجرائم أخرى وهي الالتقاط (الالتقاط الذهني) أو الاعتراض أو التنصت.

كما أن بعض التشريعات لم تقتصر على تجريم الدخول غير المشروع، بل جرمت أيضا البقاء غير المشروع[2] كالتشريع الفرنسي[3] والتشريع الامريكي[4] وكذلك التشريع الاماراتي[5] وكذلك مشروع قانون مكافحة الجرائم المعلوماتية العراقي[6]، حيث يبقى الفاعل داخل النظام المعلوماتي بعد الدخول إليه خطأ أو صدفة[7]، ويتحقق البقاء غير المشروع ممن له حق الدخول ويتجاوز ذلك بدخوله إلى جزء غير مسموح له بالدخول إليه[8]، وتطبيقا لذلك قضت محكمة استئناف باريس في حكمها الصادر في 1999/4/5 أن البقاء غير المشروع داخل النظام المعلوماتي يتحقق سواء كان الدخول نتيجة خطأ الفاعل أو أنه فقد مشروعية البقاء بعد أن كان دخوله مشروعا نتيجة خطأ من جانبه[9].

ويفرق جانب من الفقهاء بين الدخول غير المشروع والبقاء غير المشروع،

---

(1) د. أحمد محمود مصطفى، مرجع سابق، ص 109 وما بعدها. د. عبد الفتاح بيومي حجازي، الجرائم المستحدثة....، مرجع سابق، ص 486.

(2) البقاء غير المشروع يقصد به (التواجد داخل نظام المعالجة الالية للمعطيات ضد أرادة من له الحق في السيطرة على هذا النظام) ينظر: د. عبد الفتاح بيومي حجازي، مكافحة جرائم الكومبيوتر...، مرجع سابق، ص 360.

(3) ينظر: (الفقرة 1 من المادة 323) من قانون العقوبات الفرنسي.

(4) ينظر: (الفقرة أ/4 من المادة 1030) من قانون أساءة أستخدام الحاسب الفدرالي الامريكي.

(5) ينظر: المادة (2) من قانون مكافحة جرائم التقنية الاماراتي.

(6) ينظر: (الفقرة 1 من المادة 3) من مشروع قانون الجرائم المعلوماتية العراقي.

(7) د. أيمن عبد الله فكري، مرجع سابق، ص 203.

(8) د. عبد الفتاح بيومي حجازي، التجارة الالكترونية وحمايتها القانونية، مرجع سابق، ص 340.

(9) أشار اليه: د. حسين بن سعيد الغافري، مرجع سابق، ص 354 ومابعدها.

لاختلاف الطبيعة القانونية لهما فالاول جريمة ايجابية وقتية، في حين أن الثاني جريمة سلبية مستمرة، كما أن دخول النظام بموافقة المسؤول عنه والبقاء فيه بعد الوقت المسموح به لا يعد بقاء غير مشروع، و إنما سرقة وقت الحاسب الآلي أو تجاوز للصلاحيات[1].

في حين يرى جانب آخر أن هنالك تعدداً معنوياً بين الدخول غير المشروع أو البقاء غير المشروع، ويذهب آخر الى القول بأنه تعدد مادي، والذي يتحقق متى ما كان الجاني مسموح له بالدخول للنظام المعلوماتي أو تجاوز المدة المحددة، حيث أن الركن المادي للجريمة يتحقق بفعل الدخول غير المشروع أو البقاء غير المشروع أو الاثنان معا[2].

مما تقدم نخلص أن الدخول غير المشروع يستتبعه حكما البقاء غير المشروع، وهو بذلك جريمة مستقلة عن البقاء غير المشروع، لأن الأخيرة قد تكون نتيجة الدخول بطريق الخطأ أو الصدفة، أو عن طريق الدخول المشروع والبقاء بعد انتهاء الوقت المسموح، على اعتبار أن الدخول هو سلوك أولي (مفتاح لجرائم أخرى) تقع بعده العديد من الجرائم المعلوماتية، كالتجسس المعلوماتي أو الغش المعلوماتي أو السرقة المعلوماتية أو الإتلاف المعلوماتي أو استخدام النظام رغم انتهاء عقد المستخدم...الخ، واستند في ذلك الى أن فكرة الدخول غير المشروع غير محددة من ناحية الزمان[3]، كما أن تجريم البقاء غير المشروع ليس بسبب الدخول إلى النظام المعلوماتي صدفةً، وإنما بسبب البقاء داخل نظام معلوماتي يعلم الفاعل بأنه غير

(1) د. أحمد محمود مصطفى، مرجع سابق، ص 256. حمزة بن عفون، مرجع سابق، ص 122. د. حسين بن سعيد الغافري، مرجع سابق، ص 354 ومابعدها.

(2) للمزيد: د. عبد الفتاح بيومي حجازي، الجرائم المستحدثة...، مرجع سابق، ص 485 وما بعدها. د. سمية عكور، الجرائم المستحدثة في ظل التغيرات والتحولات الاقليمية والدولية، ورقة علمية مقدمة الى الملتقى العلمي (الجرائم المعلوماتية وطرق مواجهتها قراءة في المشهد القانوني والامني)، كلية العلوم الاستراتيجية، الاردن، 2014، ص 9.

(3) د. أيمن عبد الله فكري، مرجع سابق، ص 204.

مصرح له به وهو سلوك ذات طبيعة إيجابية، ولا يمثل السلوك السلبي لجريمة الدخول غير المشروع كما يدعي جانب من الفقهاء و إنما جريمة مستقلة[1].

ومن الجدير بالذكر لم تشترط أغلب القوانين وسيلة لارتكاب الجريمة المعلوماتية، حيث جاءت(الفقرة 1 من المادة 323) من قانون العقوبات الفرنسي خاليا من أية وسيلة، وعلى المسار نفسه جاء القانون الفدرالي الامريكي في المادة (1030)، وأيضا مرسوم قانون مكافحة جرائم تقنية المعلومات الاماراتي في المادة (4)، و أيضا النظام السعودي لم يحدد وسيلة معينة في (الفقرة 2 من المادة 7)، وأيضا المادة (3) من مشروع الجرائم المعلوماتية العراقي، وبالتالي يمكن ارتكابها عن طريق الدخول باستخدام كلمة السر[2] أو الرقم الكودي أو استخدام برنامج أو شفرة خاصة، أو من خلال شخص مسموح له بالدخول سواء تم ذلك عن طريق شبكات الاتصالات التلفونية أو محطات طَرفيةَ محلية أو عالمية[3].

ومن الجدير بالذكر أيضا تشترك جريمة الدخول غير المشروع مع جريمة الاعتراض أو الالتقاط أو التنصت المعلوماتي، بالوسائل المستخدمة لارتكاب الجريمة وهي عديدة منها، عن طريق الشبكة المعلوماتية، أو إحدى أجهزة الحاسب الآلي أو النظام المعلوماتي[4]، ولم يحدد التشريع الفرنسي[5] والتشريع الامريكي[6] وجاء التشريع الاماراتي[7] رغم تحديد بعض الوسائل إلا أنه استخدم عبارة " أية

---

(1) د. حسين بن سعيد الغافري، مرجع سابق، ص 356.

(2) للمزيد عن كلمة السر ينظر، ص (50 - 52) من الرسالة.

(3) د. خالد ممدوح أبراهيم، الجرائم المعلوماتية، مرجع سابق، ص 268.

(4) ينظر(الفقرة 1 من المادة 3) وكذلك (الفقرة 2 من المادة 7) من نظام مكافحة الجرائم المعلوماتية السعودي. والمادة (21) من مرسوم قانون جرائم تقنية المعلومات الاماراتي. و(الفقره ز من المادة 14) من مشروع قانون الجرائم المعلوماتية العراقي.

(5) ينظر (الفقرة 1 من المادة 226) وكذلك (الفقرة 1 من المادة 323) من قانون العقوبات الفرنسي.

(6) ينظر (الفقرة أ من المادة 1030) من قانون أساءة أستخدام الحاسب الفدرالي الامريكي.

(7) المادة (4) من مرسوم جرائم تقنية المعلومات الاماراتي.

وسيلة تقنية" وبالتالي يمكن أن ترتكب جريمة التجسس المعلوماتي بمختلف صورها، بأي وسيلة ومنها أبواب المصيدة (الابواب الخلفية أو الخفية) وهي ممرات خالية متروكة في برنامج ما، فالبرامج في نسختها الاولى تحوي على ثغرات وعيوب فنية معينة، أو أن هذه الثغرات قد تركت عمدا من قبل صانعو هذه البرامج، لينفذوا من خلالها الى النظام المعلوماتي للتجسس على معلومات المؤسسات، ولتجنب ذلك يقوم المبرمجون الماهرون باجراء تعديلات في الشفرات والمنافذ الوسطية للتخلص من تلك العيوب[1]، أو استخدام البرامج الضارة[2] للتجسس كحصان طروادة مثلا والذي يقوم بتسجيل أي حركة يقوم بها المجني عليه على لوحة المفاتيح ومن ثم الدخول إلى البيانات السرية أو الحسابات المالية أو المحادثات أو برنامج البوت والذي هو عبارة عن برنامج صغير يقوم بفتح قناة خلفية سرية بين جهاز الحاسب المستهدف وبين حاسب الفاعل يستطيع من خلاله التحكم بحاسب الضحية، وهنالك لاقطة أجهزة(الانسرماشين) التي تلتقط الرسائل لأي شخص يستخدم هاتف(الانسرماشين)، كما هنالك جهاز طوره جهاز الامن القومي الامريكي والذي يستطيع التقاط رسائل البريد الالكتروني الصادرة والواردة، وغيرها من البرامج التي تستخدم من قبل القراصنة لاختراق منظومة الاتصالات العالمية، كما ترتكب جرائم التجسس المعلوماتي بأسلوب تفجير الموقع المستهدف وذلك بإرسال كم هائل من الرسائل الى حواسيب المؤسسات وبالأخص المؤسسات المالية، ومن ثم الدخول إلى هذه الحواسيب أو خلق أرقام بطاقات الائتمان[3].

(1) د. محمد علي العريان، مرجع سابق، ص 79. د. أيمن عبد الحميد عبد الحفيظ سليمان، مرجع سابق، ص 156.

(2) للمزيد عن البرامج المستخدمة للتجسس ينظر ص(27 - 38) من الرسالة.

(3) للمزيد عن هذة الطرق والبرامج ينظر: د. حسين بن سعيد الغافري، مرجع سابق، ص 277 وما بعدها. وكذلك: د. يوسف حسن يوسف، مرجع سابق، ص 104. د. خالد ممدوح أبراهيم، فن التحقيق...، مرجع سابق، ص 344 وما بعدها. د. سليمان أحمد فضل، مرجع سابق، ص 215. حمزة بن عفون، مرجع سابق، ص 139 وما بعدها. ممدوح الشيخ، مرجع سابق، ص 70 ومابعدها.

ثانيا: النتيجة الجرمية:

هي أثر للسلوك الإجرامي و لها مدلولان أحدهما قانوني والآخر مادي، فبالنسبة للمدلول القانوني هو الاعتداء على مصلحة أو حق يحميهما القانون، وأما المدلول المادي فهو التغير الحاصل بالعالم الخارجي كأثر للسوك الاجرامي[1].

وتعتبر جريمة الدخول غير المشرع جريمة شكلية وبالتالي لا تتطلب تحقق نتيجة معينة، فليس من الضروري أن يصل الفاعل الى المعلومات أو البرامج ليتحقق الركن المادي في هذه الجريمة، لأن العلة من تجريم الدخول غير المشروع هو حماية المعلومات والبرامج من الوصول إليها ومن ثم التلاعب فيها بالمحو أو التعديل أو الافشاء...الخ[2]، وهذا ما أخذ به قانون العقوبات الفرنسي الجديد في (الفقرة 1 من المادة 323) أذ عاقب بالحبس لمدة سنة وغرامة مقدارها(100، 000) فرانك على مجرد الدخول للنظام المعلوماتي بطريق الغش.

واعتبر ترتب نتيجه ظرفا مشدداً حيث نصت على أن "... فإذا نجم عن هذا الدخول محو أو تعديل في المعطيات المخزونة في النظام أو إتلاف تشغيل هذا النظام تكون العقوبة الحبس لمدة سنتين وغرامة مقدارها (200000) فرانك ".

وعلى ذات النهج سار المشرع الاماراتي حيث عاقب على الدخول المجرد، وشدد العقوبة في حال ما إذا ترتب على الدخول دون وجه حق، نشر البيانات أو المعلومات السرية الخاصة بالحكومة أو المؤسسات أو الشركات المالية والتجارية والاقتصادية.

---

(1) د. محمد صبحي نجم، قانون العقوبات القسم العام (النظرية العامة للجريمة)، ط 3، دار الثقافة، عمان، 2010، ص 211.

(2) ماجد بن كريم الزارع، مرجع سابق، ص 90. د. نائلة عادل محمد فريدة قورة، مرجع سابق، ص 343. حمزة بن عفون، مرجع سابق، ص 120.

وذلك في المادة (4) من مرسوم قانون مكافحة جرائم تقنية المعلومات حيث نصت على أن " تكون العقوبة السجن مدة لا تقل عن خمس سنوات والغرامة التي لا تقل عن خمسمائة الف درهم ولا تتجاوز مليونين درهم، إذا تعرضت هذه البيانات أو المعلومات للإلغاء أو الحذف أو الاتلاف أو التدمير أو الافشاء أو التغير أو النسخ أو النشر أو إعادة النشر".

أما القانون الفدرالي الامريكي الخاص بجرائم إساءة استخدام الحاسب، فقد تعامل مع جريمة الدخول غير المشروع على وجهين الوجه الاول اعتبرها جريمة شكلية لم يتطلب فيها نتيجة جريمة كما في (الفقرة أ/1 وكذلك أ/3 من المادة 1030)، أما الوجه الثاني فإنه اشترط تحقق نتيجة جرمية في(الفقرة أ /2 من المادة 1030)، تتمثل بالحصول على معلومات تابعة لمؤسسة مالية أو ملف المستهلكين، أو أي مؤسسة أو وكالة تابعة للولايات المتحدة الامريكية، أو محتوى الاتصالات التي تتم بين الولايات أو الاتصالات الخارجية[1] **حيث نصت على أن** " الوصول عمدا إلى الحاسوب بدون ترخيص، أو تجاوز الترخيص الممنوح بقصد الحصول على معلومات واردة في سجل مالي بمؤسسة مالية، أو أن تشمل هذه المعلومات المتضمنة في ملف وكالة أو معلومات من أي حاسب محمي إذا تعلق بمحتوى اتصالات خارجية او بين الولايات ".

وعلى ذات النهج سار المشرع السعودي فقد اشترط تحقق نتيجه وهو الحصول على معلومات تمس الأمن الداخلي أو الخارجي للدولة أو الاقتصاد الوطني.

و ذلك في(الفقرة 2 من المادة 7) من نظام مكافحة الجرائم المعلوماتية السعودي لعام 2007 حيث نصت على أن " الدخول غير المشروع إلى موقع الكتروني، أو نظام معلوماتي مباشرة، أو عن طريق الشبكة المعلوماتية، أو إحدى

(1) د. حسين بن سعيد الغافري، مرجع سابق، ص 359.

أجهزة الحاسب الآلي للحصول على بيانات تمس الامن الداخلي أو الخارجي للدولة أو اقتصادها الوطني ".

وعلى نفس المسار جاء مشروع الجرائم المعلوماتية العراقي لعام 2012 **حيث نصت المادة (3) على أن** " أ - الدخول أو البقاء أو اتصال غير المشروع مع كل أو جزء من تقنية المعلومات أو الاستمرار به. ب - محو أو تعديل أو تشويه أو نسخ أو نقل أو تدمير للبيانات المحفوظة وللأجهزة والانظمة الالكترونية وشبكات الاتصال والحاق الضرر بالمشتركين والمستفيدين. ج - الحصول على معلومات حكومية سرية ".

ثالثا: العلاقة السببية:

يقصد بالعلاقة السببية (إمكانية إسناد نتيجة إلى فعل وربطها برباط وثيق، أي إرتباط السبب بالمسبب ومن ثم فهي عنصر لازم في جميع الجرائم عمدية كانت أم غير عمدية)[1].

فهي الرابطة بين السلوك الاجرامي والنتيجة الجرمية الضارة، فالعلاقة السببية تعمل على توحيد الركن المادي بعنصرية، ومن دونهما لا يسأل مرتكب الفعل إلا عن شروع وذلك عندما تكون الجريمة عمدية[2].

إن العلاقة السببية لا يكون مجال لبحثها إذا كانت جريمة الدخول غير المشروع من الجرائم الشكلية التي تتحقق بمجرد إرتكاب السلوك الاجرامي، في حين تبحث العلاقة السببية في جريمة الدخول غير المشروع باعتبارها جريمة ذات

(1) د. أحمد كامل سلامة، شرح قانون العقوبات/القسم الخاص (في جرائم الجرح والقتل العمدية وغير العمدية)، مكتبة نهضة الشرق، القاهرة، 1987، ص 21.

(2) د. علي حسين خلف و د سلطان الشاوي، المبادى العامة في قانون العقوبات، الدار العربية للقانون، بغداد، بدون سنة طبع، ص 141.

نتيجة مادية، حيث تطبق القواعد العامة في العلاقة السببية، فنصت على النتيجة الجرمية (الفقرة 1 من المادة 323) من قانون العقوبات الفرنسي الجديد، و (الفقرة أ / 2 من المادة 1030) من القانون الفدرالي الامريكي، والمادة (4) من مرسوم قانون مكافحة جرائم تقنية المعلومات الاماراتي، و (الفقرة 2 من المادة 7) من النظام السعودي لمكافحة الجرائم المعلوماتية، و (الفقرة ب، ج من المادة 3) من مشروع قانون الجرائم المعلوماتية العراقي.

الفرع الثاني

الركن المعنوي

لا يكفي لقيام الجريمة تحقق الركن المادي فحسب بل لا بد من أن يكون الفعل أو الامتناع وليد إرادة حرة، وتكون الارادة الحرة صادرة ممن يملك أهلية جنائية وهي ما تعرف بالأرادة[1] أو التمييز، حيث تتجه إرادة الجاني إلى إرتكاب خطأ مقصود فتقوم الجريمة العمدية أو خطأ غير مقصود وحينها تنشأ الجريمة غير عمدية، فالقصد الجرمي[2] يتحقق بإرادة الفعل وإرادة النتيجة التي حققها السلوك، إضافة الى العلم[3] بأركان الجريمة كما عرفها القانون، ويشترط بالعلم الذي هو أحد عناصر الركن المعنوي أن يكون معاصرا لفعل الدخول واتجاه الارادة لإرتكاب الفعل[4]، فالإرادة تعد عنصرا لازماً لقيام الركن المعنوي[5].

فالتشريعات التي لم تتطلب قصدا خاصة و التي عاقبت على الدخول المجرد هي قانون العقوبات الفرنسي الجديد في (الفقرة أ من 323) والذي تطلب أن يتم الدخول أو البقاء بطريق الغش أو الخداع[6]، وبهذا التصور لا تقع جريمة الدخول

(1) يقصد بالارادة: (هي عبارة عن قوة نفسية من شأنها الخلق والسيطرة فهي تخلق فكرة الجريمة وبعد ذلك يأتي دور السيطرة في مرحلة التنفيذ، ففي مرحلة التفكير في الجريمة يكون لها دور نفسي يدخل في حيثيات الركن المعنوي، أما في دور التنفيذ فهي تدخل في حيثيات الركن المادي بوصفها عنصراً فيه). للمزيد: محروس نصار الهيتي، مرجع سابق، ص 107 - 108.

(2) عرفت (الفقرة 1 من المادة 33) من قانون العقوبات العراقي القصد الجرمي بأنه (هو توجيه الفاعل أرادته الى أرتكاب الفعل المكون للجريمة هادفا الى النتيجة الجرمية التي وقعت أو أي نتيجة جرمية أخرى).

(3) العلم يقصد به: (الاحاطة بالشئ، أو أدراك الامور على نحو صحيح مطابق للواقع). للمزيد: محروس نصار الهيتي، مرجع سابق، ص 95.

(4) ماجد بن كريم الزارع، مرجع سابق، ص 89. حمزة بن عفون، مرجع سابق، ص 121.

(5) د. مصطفى يوسف، أصول المحاكمات الجنائية، دار النهضة العربية، القاهرة، 2008، ص 49.

(6) د. حسام محمد نبيل الشنراقي، مرجع سابق، ص 169.

أو البقاء في التشريع الفرنسي الا عمدية، وكذلك لم يطلب قصدا خاصا القانون الفدرالي الامريكي الخاص بأساءة أستخدام الحاسبات الآلية في (الفقرات أ /3/1 من المادة 1030) في حال الدخول الى حواسيب الحكومة أو حواسيب متعلقة بأعمال الحكومة، وكذلك لم يشترط قصدا خاص المرسوم بالقانون الاتحادي الاماراتي لمكافحة جرائم تقنية المعلومات في المادة (4) فأنه جرم الدخول المجرد للنظام المعلوماتي أو موقع الكتروني...الخ، بغض النظر عن قصد الفاعل سواء كان قصده الحصول على معلومات حكومية أو معلومات سرية تخص التجارة أو الاقتصاد...الخ، وعلى نفس المسار جاءت المادة (3) من مشروع قانون الجرائم المعلوماتية العراقي.

وهنالك من لم يكتفِ بالقصد الجرمي لقيام هذه الجريمة، وهو العلم بأنه غير مصرح له بالدخول واتجاه إرادته إلى إرتكاب فعل الدخول، بل لابد من قصد خاص يتمثل بنية ارتكاب جريمة لاحقة لفعل الدخول وهو إتجاه القانون الانكليزي[(1)]، ومن التشريعات التي أخذت بذلك التشريع الامريكي حيث استلزمت(الفقرة أ /4/2 من المادة 1030) على القصد الخاص وهو قصد الحصول على معلومات متعلقة بالمؤسسات المالية أو ملفات المستهلكين أو محتوى الاتصالات الداخلية أو الخارجية، أو بقصد الحصول على معلومات تخص مؤسسات أو وكالات تابعة للولايات أو تعديلها، ومن الجدير بالذكر لم يتناول المشرع الامريكي حالات الدخول إلى الحاسب التي تكون نتيجة خطأ من الفاعل، بل الحالات التي يكون فيها الدخول مصرح به أبتداءا ويتجاوز الفاعل التصريح الممنوح له[(2)].

وقد سار على نفس الاتجاه المشرع السعودي في (الفقرة 2 من المادة 7) حيث اشترط أن يكون الى جانب القصد العام قصد خاص، هو قصد الفاعل من

(1) د. نائلة عادل محمد فريد قورة، مرجع سابق، ص 370.

(2) د. حسين بن سعيد الغافري، مرجع سابق، ص 360.

الدخول غير المشروع الحصول على معلومات تخص الأمن الداخلي أو الخارجي أو الاقتصاد الوطني السعودي[1].

فالركن المعنوي لا يقوم ولا تقوم الجريمة في حال كان الدخول بناءً على خطأ الفاعل أو أعتقد أن من حقه الدخول بشرط الخروج مباشرةً عند علمه بأنه ليس مسموح له بذلك[2]، وهو أمر غير متوقع في التشريع الفرنسي لأنه الدخول المجرم حسبما جاء فيه هو الذي يتم بالغش أو الخداع، وأرى أن من الافضل الاكتفاء بالقصد الجرمي العام في تجريم الدخول غير المشروع، واستند في ذلك إلى أنه متى ما توافر القصد الجرمي بعنصرية العلم والإرادة فلا محل للباعث على ارتكاب الجريمة سواء كان الباعث سياسي أو عسكري أو تجاري أو غير ذلك[3].

(1) عبد الله بن محمد كريري، الركن المعنوي في الجرائم المعلوماتية في النظام السعودي، رسالة ماجستير، جامعة نايف العربية للعلوم الامنية، الرياض، 2013، ص 122.

(2) د. عبد الفتاح بيومي حجازي، الجرائم المستحدثة...، مرجع سابق، ص 487.

(3) د. حسين بن سعيد الغافري، مرجع سابق، ص 357.

الفرع الثالث

الركن المفترض (المحل)

اختلف محل الجريمة باختلاف التشريعات محل الدراسة المقارنة، ففي التشريع الفرنسي فأن محل الجريمة هو نظام المعالجة الآلية للبيانات نفسه أو المعطيات المخزونة أو الشبكات المعلوماتية استنادا الى (الفقرة 1 من المادة 323)، حيث شملت الحماية الى جانب المعطيات الأجهزة الالكترونية والأنظمة التي تعمل بها هذه الاجهزة[1]، أما التشريع الفدرالي الأمريكي فإن محل الجريمة هو المعلومات المحظورة الخاصة بالطاقة الذرية والتي ذكرتها المادة (11) من قانون الطاقة الذرية لعام 1954، أو المعلومات الموجودة داخل حواسيب المؤسسات المالية أو مؤسسات أو وكالات الولايات المتحدة الامريكية الحكومية أو التي تعمل لأجل أو لصالح الحكومة الامريكية، وكذلك محتوى الاتصالات الداخلية أو الخارجية استنادا للمادة (1030) من القانون الفدرالي الامريكي الخاص بجرائم استخدام الحاسب لعام 1984 المعدل، أما التشريع الاماراتي فإن محل الجريمة هو المواقع الالكترونية أو النظام المعلوماتي الالكتروني أو الشبكة المعلوماتية أو أن يكون المحل هو أية وسيلة من وسائل تقنية المعلومات استنادا الى المادة (4) من مرسوم قانون مكافحة جرائم تقنية المعلومات لعام 2012، حيث نجد المشرع الاماراتي جعل الباب مفتوحاً عندما ذكر عبارة "أو أية وسائل تقنية" وهو أمر مستحسن من وجهة نظري، أما النظام السعودي فقد حدد محل الجريمة بأنه موقع الكتروني أو نظام معلوماتي استنادا إلى (الفقرة 2 من المادة 7) من النظام السعودي لمكافحة الجرائم المعلوماتية لعام 2007. أما مشروع قانون الجرائم

(1) أحمد بن زايد جوهر الحسن المهندي، مرجع سابق، ص 136.

المعلوماتية العراقي، فأن محل الجريمة هو تقنية المعلومات والانظمة الالكترونية وشبكات الاتصال والبيانات المحفوظة داخلها أو المتداولة عن طريقها والمعلومات الحكومية السرية، استنادا إلى المادة (3) من المشروع.

ومن الجدير بالذكر أن محل الحماية لا يقتصر على النظام المعلوماتي أو الموقع الالكتروني أو الشبكة المعلوماتية، بل يشمل البيانات بمعناها الواسع والتي تشمل(البيانات العسكرية، بيانات العملاء في البنوك، البيانات الصناعية، البيانات الشخصية، برامج الحاسب، وكذلك الصور أو الأوامر أو الأصوات أو الرسائل أو الارقام والحروف والرموز وكل مايمكن تخزينة ومعالجته ونقله وإنشاؤة بواسطة الحاسب الآلي وغيرها)، كما يشمل المحل أنظمة الحاسوب غير المرتبطة بالشبكات أو الشبكات نفسها[1]، فالمحل يشمل البيانات أو المعلومات الخاصة أو العامة، حيث يكون محل التجسس المعلوماتي الخاص، هو الأختراق أو الاطلاع على البيانات أو المعلومات والمراسلات المحجوبة عن الآخرين والتي يجب أن تبقى سرية[2]، أما التجسس المعلوماتي العام فيضاف الى ماتقدم نقل أو تسليم البيانات السرية المحجوبة والتي تخص البيانات الحكومية[3] السرية والتي لها مساس بأمن الدولة الخارجي أو الداخلي أو اقتصادها الوطني الى العدو لكي يستفيد منها في زمن السلم أو الحرب[4].

(1) د. نائلة عادل محمد فريد قورة، مرجع سابق، ص 315 وما بعدها. د. خالد ممدوح أبراهيم، الجرائم المعلوماتية، مرجع سابق، ص 258 - 259. نهلا عبد القادر المومني، مرجع سابق، ص 217. وكذلك: (الفقرة 4 من المادة 1) من النظام السعودي لمكافحة الجرائم المعلوماتية.

(2) ماجد بن كريم الزارع، مرجع سابق، ص 90.

(3) يقصد بالبيانات الحكومية بأنها(البيانات الخاصة بالحكومة الاتحادية والحكومات المحلية والهيأت العامة والمؤسسات العامة والاتحادية والمحلية) ينظر: المادة (1) من قانون مكافحة الجرائم المعلوماتية الاماراتي.

(4) سورية بنت محمد الشهري، مرجع سابق، ص 38. د. عبد الفتاح بيومي حجازي، جرائم الكومبيوتر والانترنت في التشريعات العربية، مرجع سابق، ص 215 وما بعدها.

نخلص مما تقدم أن محل جريمة الدخول غير المشروع هو أما الشبكة المعلوماتية[1]، أو أجهزة الحاسب الآلي[2]، أو النظام المعلوماتي[3]، أو الموقع الالكتروني[4]، أو أحدى وسائل تقنية المعلومات، أو البيانات أو المعلومات أو البرامج أو الصور أو محتوى الاتصالات أو الرسائل البريدية أو البرقية..الخ.

(1) الشبكة المعلوماتية يقصد بها(أرتباط اكثر من حاسب آلي أو نظام معلوماتي، للحصول على البيانات وتبادلها، مثل الشبكات الخاصة والعامة والشبكات العالمية).ينظر: (الفقرة 3 من المادة 1) من نظام مكافحة جرائم المعلومات السعودي.

(2) الحاسب الآلي يقصد بها(أي جهاز الكتروني ثابت أو منقول، سلكي أو لا سلكي يحتوي على نظام معالجة البيانات، أو تخزينها أو أرسالها، أو أستقبالها أو تصفحها، يؤدي وظائف محددة بحسب البرامج والاوامر المعطاة له).ينظر: (الفقرة 6 من المادة 1) من نظام مكافحة جرائم المعلومات السعودي.

(3) النظام المعلوماتي يقصد به:(مجموعة من البرامج وأدوات معدة لمعالجة وأدارة البيانات أو المعلومات أو الرسائل الالكترونية أو غير ذلك). ينظر: المادة (1) من القانون الاتحادي الاماراتي لمكافحة جرائم تقنية المعلومات.

(4) الموقع الالكتروني يقصد به (هو مكان أتاحة البيانات على الشبكة المعلوماتية من خلال عنوان محدد). ينظر: (الفقرة 9 من المادة 1) من النظام السعودي لمكافحة الجرائم المعلوماتية.

المطلب الثاني

عقوبة جريمة الدخول غير المشروع

سنتناول في هذا المطلب العقوبات الأصلية والعقوبات الفرعية التي يحكم بها على مرتكبي جريمة الدخول غير المشروع وذلك بفرعين وعلى النحو الاتي.

- **الفرع الاول:** العقوبات الأصلية.
- **الفرع الثاني:** العقوبات الفرعية.

الفرع الاول

العقوبات الأصلية

عاقب المشرع الفرنسي على جريمة الدخول غير المشروع في (الفقرة 1 من المادة 323) بالحبس لمدة سنة وغرامة مقدارها(100، 000) فرانك، وقد شدد العقوبة إذا نجم عن هذا الدخول محو أو تعديل في المعطيات المخزونة في النظام أو إتلاف تشغيل هذا النظام، حيث تكون العقوبة الحبس لمدة سنتين وغرامة مقدارها (200، 000) فرانك. ومن الجدير بالذكر هو أن قانون العقوبات الفرنسي في المادة (131) منه قد اعتبر المصادرة عقوبة أصلية وليست عقوبة تكميلية.

أما بالنسبة للمشرع الامريكي فقد عاقب على الدخول المجرد إلى جهاز الحاسب الآلي بالسجن لمدة لاتزيد عن عشر سنوات أو الغرامة او بكلتا العقوبتين في (الفقرة أ /1/من المادة 1030) وتكون العقوبة السجن لمدة لاتزيد عن سنة واحدة أو الغرامة أو بكلتا العقوبتين في (الفقرة أ /3/ من المادة 1030)، وتكون العقوبة هي السجن لمدة لا تزيد عن خمس سنوات أو الغرامة أو بكلتا العقوبتين للأفعال المرتكبة في (الفقرة أ /4/2 من المادة 1030)، والتي تكون بقصد الحصول على معلومات واردة في سجل مالي بمؤسسة مالية، أو أن تشمل هذه المعلومات المتضمنة في ملف وكالة أو معلومات من أي حاسب محمي إذا تعلق بمحتوى اتصالات خارجية أو بين الولايات.

في حين قرر المشرع السعودي لهذه الجريمة في (الفقرة 2 من المادة 7) من نظام مكافحة الجرائم المعلوماتية، عقوبة الحبس لمدة لا تزيد على عشر سنوات و بغرامة لا تزيد على خمسة ملايين ريال سعودي أو إحدى هاتين العقوبتين. ما يأخذ على المشرع السعودي أنه لم يجرم الدخول المجرد إلى النظام المعلوماتي أو الموقع

الالكتروني، كما لم يجعل من الحصول على البيانات التي تمس أمن الدولة ظرفاً مشدداً.

أما المشرع الاماراتي فقد عاقب على هذه الجريمة في المادة (4) من مرسوم مكافحة جرائم تقنية المعلومات، حيث عاقب على الدخول المجرد بالسجن المؤقت والغرامة التي لا تقل عن مائتين وخمسين ألف درهم ولا تتجاوز مليون وخمسمائة الف درهم، كل من دخل بدون تصريح إلى موقع الكتروني، او نظام معلوماتي الكتروني، أوشبكة معلوماتية، أوسيلة تقنية معلومات، سواء كان الدخول بقصد الحصول على بيانات حكومية، أو معلومات سرية خاصة بمنشأة مالية أو تجارية أو اقتصادية. وقد شدد العقوبة الى السجن مدة لا تقل عن خمس سنوات والغرامة التي لا تقل عن خمسمائة الف درهم ولا تتجاوز مليونين درهم، إذا تعرضت هذه البيانات أو المعلومات للإلغاء أو الحذف أو الإتلاف أو التدمير أو الإفشاء أو التغيير أو النسخ أو النشر أو إعادة النشر.

أما مشروع قانون الجرائم المعلوماتية العراقي لعام 2012 جاء خاليا من العقوبات، حيث وردت فيه عبارة (الاحكام العقابية بحاجة الى مناقشة من قبل القانونيين)، أما مشروع قانون الجرائم المعلوماتية لعام 2010 جاء متضمناً عقوبات ولكن لم يجرم الدخول أو البقاء غير المشروع.

الفرع الثاني

العقوبات الفرعية(1)

سنتناول في هذا الفرع العقوبات التكميلية والتدابير الاحترازية دون العقوبات التبعية لأنها لا تلحق المحكوم عليه في التشريعات المقارنة، أما في التشريع العراقي فنظرا لعدم إقرار مشروع قانون الجرائم المعلوماتية وخلوه من عقوبة أصلية، وبالتالي لا يمكن أن نحدد إذا كانت تلحق بالمحكوم عليه من عدمه.

أولا: العقوبات التكميلية(2):

إن العقوبات التكميلية في التشريع الفرنسي والتي أجاز القانون للمحكمة أن تفرضها في الجنايات والجنح، إلى جانب العقوبات الأصلية المنصوص عليها للجرائم المعلوماتية، هي الحرمان من الحقوق المدنية المتعلقة بالأسرة لمدة خمس سنوات حسب المواد (26 - 131) من قانون العقوبات، كذلك الحرمان من شغل الوظائف العامة أو الانشطة المهنية، أو الاجتماعية إذا كانت الجريمة قد ارتكبت بسببها أو بمناسبة مباشرتها، وكذلك يجوز للمحكمة مصادرة الأشياء المستخدمة في الجريمة أو المعدة للاستخدام فيها أو المتحصلة منها عدا التي تكون محلا للرد، وكذلك إغلاق الأماكن والمشروعات التي استخدمت في ارتكاب الجريمة لمدة لاتزيد عن خمس سنوات، وأيضا إبعاد المحكوم عليه عن الأسواق العامة لمدة لا تزيد عن

(1) نصت (الفقرة ه من المادة 224) من قانون اصول المحاكمات الجزائية العراقي رقم 23 لعام 1971 المعدل على أن: (يقصد بالعقوبات الفرعية الواردة في هذا القانون، العقوبات التبعية والتكميلية والتدابير الاحترازية المنصوص عليها في قانون العقوبات).

(2) العقوبات التكميلية هي (جزاءات ثانونية تتفق مع العقوبات التبعية في أنها لا تأتي بمفردها، بل تابعة لعقوبة أصلية ولكن تختلف عنها، في أنها لا تلحق المحكوم عليه حكما وبقوة القانون، بل يجب أن ينص عيها القاضي صراحه في حكمه المتضمن للعقوبة الاصلية). ينظر: د. علي حسين خلف و د.سلطان الشاوي، مرجع سابق، ص 436.

خمسة سنوات، ومنع المحكوم عليه من إصدار الشيكات لمدة لا تزيد على خمسة سنوات، عدا تلك التي تمكن الساحب من سحب أموال المسحوب عليه أو التي تكون مقبولة الدفع، وكذلك إعلان ونشر الحكم حسب الشروط الواردة بالمادة (35 - 131) من قانون العقوبات الفرنسي[1].

أما التشريع السعودي فقد أجاز للمحكمة الحكم بمصادرة الأجهزة أو البرامج أو الوسائل المستخدمة في ارتكاب الجريمة، أو الأموال المتحصلة منها، كما للمحكمة الحكم بإغلاق مؤقت أو نهائي للموقع الالكتروني أو مكان تقديم الخدمة متى ماكان مصدرا لارتكاب الجريمة، وكانت الجريمة ارتكبت بعلم مالكه وهذه الأحكام يجوز فرضها في كل الجرائم المعلوماتية المنصوص عليها في النظام السعودي ومنها الالتقاط أو الاعتراض أو التنصت المعلوماتي [2].

أما التشريع الاماراتي الاتحادي الخاص بمكافحة جرائم تقنية المعلومات فقد ألزم المحكمة بإصدار حكم يقضي بإبعاد الأجنبي خارج البلاد في حال الحكم عليه بالحبس وفق أحكام هذا المرسم بقانون، بعد أن يتم تنفيذ العقوبة المحكوم بها[3]، وكذلك ألزم المحكمة في جميع الأحوال بإصدار أحكام تقضي بمصادرة الاجهزة أو البرامج أو الوسائل المستخدمة في ارتكاب الجريمة، أو الاموال المتحصلة منها، ومحو المعلومات أو البيانات أو إعدامها، كما يحكم بإغلاق المحل أو الموقع الذي ترتكب أياً من هذة الجرائم غلقاً كلياً أو المدة التي تحددها المحكمة [4].

(1) المادة (5/323) من قانون العقوبات الفرنسي الجديد. أشار اليها: حسام محمد نبيل الشنراقي، مرجع سابق، ص 176 - 177.

(2) المادة (10) من النظام السعودي لمكافحة الجرائم المعلوماتية.

(3) المادة (42) من مرسوم مكافحة جرائم تقنية المعلومات الاماراتي.

(4) المادة (41) من مرسوم مكافحة جرائم تقنية المعلومات الاماراتي.

ثانيا: التدابير الاحترازية:

أجاز المشرع الاماراتي في مرسوم قانون مكافحة الجرائم التقنية للمحكمة من فرض تدابير إحترازية، وذلك في نص المادة (43) ومن هذه التدابير وضع المحكوم عليه تحت الإشراف أو المراقبة أو الحرمان من استخدام شبكة المعلومات، أو نظام معلوماتي الكتروني، أو أية وسيلة تقنية أخرى، أو وضعه في مأوى علاجي، أو مركز تأهيل للمدة التي تقررها المحكمة.

المبحث الثاني

جريمة الاعتراض أو الالتقاط أو التنصت المعلوماتي

سنتناول في هذا المبحث أركان الجريمة وعقوباتها، وقبل ذلك نورد النصوص القانونية التي جرمت تلك الافعال.

فبالنسبة للتشريع الفرنسي فقد نص في (الفقرة 1 من المادة 226) من قانون العقوبات النافذ على أن " يعاقب بالحبس وبغرامة لا تزيد على ثلاثمائة الف فرنك، كل من يعتدي إراديا أو عمدا على حرمة الحياة الخاصة للغير بأي وسيلة كانت: 1 - بالتنصت أو بتسجيل أو بنقل الأحاديث التي تصدر عن شخص بصفة سرية أو خاصة دون رضاه. 2 - بإلتقاط أو تسجيل أو بنقل صورة شخص يوجد في مكان خاص دون رضاه ".

أما التشريع السعودي فقد جرم هذه الأفعال (بالفقرة 1 من المادة 3) من نظام مكافحة الجرائم المعلوماتية بالقول " التنصت على ماهو مرسل عن طريق الشبكة المعلوماتية، أو إحدى أجهزة الحاسب الآلي، دون مسوغ نظامي صحيح أو إلتقاطه أو إعتراضه ".

أما التشريع الاماراتي فقد جرم في المادة (21) من مرسوم قانون مكافحة جرائم تقنية المعلومات أفعال الالتقاط أو الاعتراض أو استراق السمع حيث نصت على أن " يعاقب بالحبس مدة لا تقل عن ستة أشهر والغرامة التي لاتقل عن مائة وخمسين ألف درهم ولا تتجاوز خمسمائة ألف درهم أو بأحدى هاتين العقوبتين، كل من استخدم شبكة معلوماتية أو نظام معلوماتي ألكتروني، أو إحدى وسائل تقنية المعلومات، في الاعتداء على خصوصية شخص في غير الأحوال المصرح بها

قانونا بإحدى الطرق التالية: 1 – استراق السمع أو اعتراض أو تسجيل أو نقل أو بث أو إفشاء محادثات أو إتصالات ومواد صوتية أو مرئية. 2 – إلتقاط صور الغير أو إعداد صور ألكترونية أو نقلها أو كشفها أو نسخها أو الاحتفاظ بها. 3 – نشر أخبار أو صور الكترونية أو صور فوتوغرافية أو مشاهد أو تعليقات أو بيانات أو معلومات ولو كانت صحيحة وحقيقية. كما يعاقب بالحبس مدة لا تقل عن سنة واحدة والغرامة التي لا تقل عن مائتين وخمسون ألف درهم ولا تتجاوز خمسمائة ألف درهم أو بإحدى هاتين العقوبتين، كل من استخدم نظام معلوماتي ألكتروني، أو إحدى وسائل تقنية المعلومات، لإجراء أي تعديل أو معالجة على تسجيل أو صورة أو مشهد، بقصد التشهير أو الإساءة إلى شخص آخر، أو الاعتداء على خصوصيته أو إنتهاكها ".

أما مشروع قانون الجرائم المعلوماتية العراقي فقد جرمت (الفقرة ز من المادة 14) فعل الالتقاط أو الاعتراض حيث نصت على أن " التقط أو اعترض بدون وجه حق ماهو مرسل عن طريق أحد أجهزة الحاسوب أو شبكة المعلومات لاستخدامها في تحقيق منفعة مالية له أو لغيره ".

المطلب الاول

الأركان العامة لجريمة الاعتراض أو الالتقاط أو التنصت المعلوماتي

سنستعرض في هذا المطلب أركان الجريمة المتمثلة بالركن المادي والمعنوي ومحل الجريمة وعلى النحو الاتي.

- **الفرع الاول:** الركن المادي.
- **الفرع الثاني:** الركن المعنوي.

الفرع الاول

الركن المادي

- سبق القول - أن الركن المادي له ثلاثة عناصر نشاط ونتيجة وعلاقة سببية وهذا ما سنوضحه تباعا.

أولا: السلوك الاجرامي:

يتخذ سلوك الجاني ثلاث صور هي الاعتراض أو الالتقاط أو التنصت المعلوماتي.

فبالنسبة للإعتراض يعرف لغة: بأنه العرض والعرض والعارض، والجمع العروض[1]، ويقال اعترضه اعتراضا فأخذ منه حاجتي[2]، ويقال اعترض الشئ دون الشئ، أي حال دونه[3].

قانونا: حددت المادة (4) من مشروع قانون الجرائم المعلوماتية العراقي، وأيضا المادة (7) من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، مفهوم الاعتراض المعلوماتي بأنه " الاعتراض المتعمد بدون وجه حق لخط سير البيانات بأي من الوسائل الفنية وقطع بث أو استقبال بيانات تقنية المعلومات ".

ويعرف أيضا حسبما حددته المذكرة التفسيرية لاتفاقية بودابست بأنه (الحصول على المحتوى الاتصالات أو بيانات الحاسب بطريقة مباشرة وذلك بالدخول الى النظام المعوماتي واستخدامه، أو بشكل غير مباشر باستخدام أجهزة

(1) الصاحب بن عباد، المحيط في اللغة، ج1، مرجع سابق، ص 49.
(2) أبن منظور، لسان العرب، ج7، ط 1، مرجع سابق، ص 199.
(3) إسماعيل بن حماد الجوهري، الصحاح في اللغة، ج1، مرجع سابق، ص 460.

التنصت لإعتراض الانبعاثات الاشعاعات الكهرومغناطيسية أو أيا من الوسائل الفنية الغير علنية)، ومن الجدير بالذكر أن الغير علنية هنا تخص الوسيلة وليس البيانات المستهدفة لأنه قد تكون الخدمة متاحة إلا أن الفاعل يرغب بالاتصال بطريقة سرية [1].

فقها: يعرف الاعتراض بأنه (رصد الاشارات الكهرومغناطيسية في الانظمة المعلوماتية وتحليلها، بهدف استرجاع المعلومات المفهومة أو المقروءة منها)[2]، وأيضا بأنه(التنصت أو نقل البيانات التي تتم داخل جهاز الحاسب، أو التي تتم عبر جهازين عن بعد عبر الشبكات المعلوماتية المختلفة، أو بترجمة الانبعاثات الكهرومغناطيسية الصادرة من الحاسب أو التي تتم عبر الاجهزة اللاسلكية وذلك عن طريق أي من الوسائل الفنية الغير علنية)[3].

فالسلوك الإجرامي في هذه الجريمة يتمثل بقيام الفاعل باعتراض الموجات اللاسلكية (الموجه الكهرومغناطيسية) التي تخص الغير، والتي تحمل البيانات أو التي تستخدم لتأمين الاتصالات[4] بدون وجه حق مستخدما وسائل فنية غير علنية[5]، كوضع شاشة عرض مثلا موصلة بجهاز تسجيل خارج المبنى المستهدف تقوم الشاشة بالتقاط الموجات الكهربائية التي تحيط بالحاسب وتحويلها الى معلومات مقروءة وتسجيلها أيضا، ويقتصر دور الفاعل هنا على التقاط المعلومات دون أن يكون له دور في تعديلها كما لا يكون له دور في تحديد المعلومات الملتقطة،

(1) المادة (3) من اتفاقية بودابست لعام 2001. للمزيد ينظر: د. هلالي عبد اللاه أحمد، مرجع سابق، ص 60 ومابعدها.

(2) د. عفيفي كامل عفيفي، مرجع سابق، ص 466.

(3) بهاء فهمي الكبيجي، مرجع سابق، ص 48.

(4) د. عبد الفتاح بيومي حجازي، الجرائم المستحدثة....، مرجع سابق، ص 191، 192. د. عماد مجدي عبد الملك، مرجع سابق، ص 170. د. محمد محمود المكاوي، مرجع سابق، ص 126.

(5) بلال أمين زين الدين، مرجع سابق، ص 306.

ولكن يكون له دور في اختيار المكان الذي يمكن فيه أن يلتقط معلومات مفيدة[1]، أو يقوم الفاعل بأستخدام فيروسات لإعتراض النظام المعلوماتي، أو يقوم الفاعل باستخدام أجهزة خاصة (لاتصدر أي إشارات) تقوم باعتراض الاتصالات بين المحطات الأرضية و الأقمار الصناعية[2]، ويتم الاعتراض كذلك بقيام الفاعل بالتقاط البيانات التي يتضمنها الاتصال الذي يتم داخل نظام حاسب واحد أو بين نظامين مختلفين أو بين عدة أنظمة معلوماتية مرتبطة ببعضها من خلال شبكة الانترنت، وهذا السلوك يشبه التنصت على المكالمات الهاتفية[3].

وتجدر الاشارة إلى أن بعض الدول تسمح باعتراض الاتصالات البعدية وكذلك شبكات تبادل المعلومات، في إطار التفتيش عن الجرائم كفرنسا مثلا في قانونها الصادر عام 1991 الخاص بالاتصلات، والتشريع الامريكي أيضا حيث أجاز اعتراض الاتصالات وشبكات الحاسب بشرط الحصول على إذن قضائي[4]، وإن كانت قد عملت وكالة الاستخبارات الامريكية FBI)) وبالتعاون مع شركة ميكروسوفت باعتراض البيانات لأغراض تجسسية[5]، كما سمح بذلك التشريع الاردني بموجب نص المادة (76) والمادة (80) إذ كان الهدف من اعتراض الرسائل أو الموجات الراديوية لمنع وقوع جريمة[6].

---

(1) د. احمد محمود مصطفى، مرجع سابق، ص 257 وما بعدها.

(2) نهلا عبد القادر المومني، مرجع سابق، ص 217 وما بعدها. د. أيمن عبد الحفيظ عبد الحميد، مرجع سابق، ص 156.

(3) د. احمد محمود مصطفى، مرجع سابق، ص 110.

(4) د. عبد الفتاح بيومي حجازي، الجوانب الاجرائية... مرجع سابق، ص 657.

(5) جيلين جرينوالد، ترجمة بسام شيحا، لا مكان للأختباء، ط 1، الدار العربية للعلوم ناشرون، بيروت، 2014، ص 145 وما بعدها.

(6) أشارة اليه: محمد أمين الرومي، مرجع سابق، ص 187 ومابعدها.

أما الإلتقاط المعلوماتي لغة: يأتي بمعنى لقط الشئ أو الصورة، ولقلط والتقطه والمفعول ملقوط، ويقال لكل ساقطة لاقطة، أي لكل ما ندر من الكلام من يسمعه ويذيعه [1]، ويقال فلان يلتقط كلام الناس ويدعى النمام، ويدعى أيضا لقيطي[2].

قانونا: يقصد بالالتقاط المعلوماتي بأنه " مشاهد البيانات او الحصول عليها دون مسوغ نظامي صحيح" [3]، **ويعرف أيضا** " مشاهدة البيانات أو المعلومات أو الحصول عليها "[4].

فقها: يعرف الالتقاط الذهني بأنه(عملية التقاط المعلومات التي تظهر على شاشة الحاسب من قبل أشخاص غير مخولين، وذلك لوضعية الجهاز غير السليمة [5]، أي الاستحواذ البصري على البيانات بحيازتها والتقاطها بصريا و ذهنيا من الشاشة) [6].

أما التقاط الموجات الكهربائية فيعرف بأنه (عملية جمع المعلومات عن بعد والتي يتم إرسالها من خلال النظام المعلوماتي داخل مبنى باستخدام شاشة عرض يتم توصيلها بجهاز تسجيل خارج المبنى، يقوم بالتقاط الموجات الكهربائية التي تنبعث من الحاسب الآلي والتي تتحول لمعلومات معروضة على الشاشة والقيام

(1) إسماعيل بن حماد الجوهري، تحقيق أحمد عبد الغفور عطار، الصحاح في اللغة، ج 2، مرجع سابق، ص 146.

(2) أبراهيم مصطفى وأخرون، المعجم الوسيط، ج 2، ص 834.محمد بن مكرم بن منظور الأفريقي المصري، لسان العرب، ج 7، ط 1، مرجع سابق، ص 392.

(3) المادة (10/1) من نظام مكافحة جرائم المعلوماتية السعودي.

(4) ينظر: (الفقرة 8 من المادة 2) من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات. وكذلك:المادة (1) من مرسوم مكافحة جرائم تقنية المعلومات الاماراتي.

(5) د.محمد محمود المكاوي مرجع سابق، ص 254.

(6) د.عبد الفتاح بيومي حجازي، نحو صياغة....، مرجع سابق، ص62. د احمد محمود مصطفى، مرجع سابق، ص248.

بتسجيلها أيضا)[1]. وهنالك اختلاف جوهري بين الالتقاط الذهني وبين الالتقاط الموجات الكهربائية، حيث أن الاول يحدد المعلومات المراد التقاطها، في حين أن إلتقاط الموجات وإن كان يحدد الفاعل المكان المراد التقاط الموجات فيه لكن لا يستطيع تحديد المعلومات أو البيانات الملتقطة.

يتخذ السلوك الإجرامي في الالتقاط المعلوماتي عدة صور منها إلتقاط الشفرة، و التقاط المعلومات عن بعد أو مابين الحاسب الآلي والنهاية الطرفية، أو بالالتقاط الذهني مباشرةً أو باستخدام الكامرات، حيث لا يتطلب السلوك الاجرامي للإلتقاط الدخول في النظام المعلوماتي للحصول على البيانات أو المعلومات، بل يتم بالتقاط الذبذبات المغناطيسية[2].

فبالنسبة لإلتقاط الشفرة يتمثل السلوك الأجرامي بالتقاط الاشعاعات الخارجة من الجهاز المعلوماتي ثم تسجيل هذه البيانات وحل شفرتها بواسطة أجهزة متخصصة، حيث تصدر الطابعات أثناء اشتغالها اشعاعات كهرومغناطيسية فيتم ربط الطابعات المستخدمة في إرتكاب الجريمة مع طابعات النظام المستهدف باستخدام جهاز صغير مهمته التقاط هذه الاشعاعات وتسجيلها وتحويلها إلى معلومات[3].

أما عن التقاط المعلومات عن بعد أو مابين الحاسب الآلي والنهاية الطرفية، وذلك بالدخول غير المشروع في النظام المعلوماتي بواسطة طرفية بعيدة، إذ يقوم الفاعل بإلتقاط المعلومات الموجودة مابين الحاسب والنهاية الطرفية من خلال

(1) د. حسام محمد نبيل الشنراقي، مرجع سابق، ص 165.

(2) د. سمية عكور، مرجع سابق، ص 7.

(3) محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة، الاسكنرية، 2004، ص 75 ومابعدها. وكذلك: غراهام يوست، ترجمة الياس فرحات، تكنولوجيا التجسس، دار الحرف= =العربي، بيروت، بدون سنة طبع، ص 225. د. عمر ابو الفتوح عبد العظيم الحمامي، مرجع سابق، ص 226 - 227.

وضع خطوط تحويلية، والتي تقوم بأرسال إشارات الكترونية للمعلومات المخترقة إلى النهاية الطرفية المتجسسة[1]، وأرى هنا تشابهاً مابين الالتقاط المعلوماتي والدخول غير المشرع، كما تستخدم برامج صغيرة مثل برنامج (كويكز وكذلك برنامج الشم) الذي يستطيع التقاط المعلومات السرية والخاصة، والذي استخدمته كثير من الدول للتجسس على المعارضين السياسين[2]، أو يكون بالتقاط المكالمات الهاتفية أو المعلومات المتداولة عن طريق شبكة الاتصالات العامة في غير الاحوال المشروعة قانونا، بأستخدام هوائيات تربط بحاسب خاص والتي تقوم بألتقاط الموجات الكهرومغناطيسية المنبعثة من الحواسيب أثناء تشغيلها من على بعد ثلاثمائة قدم من الحاسب المستهدف[3].

أما الالتقاط الذهني البصري المباشر أو باستخدام الكاميرات، فأن السلوك الاجرامي يتم بالالتقاط الذهني البصري وذلك بوضع كاميرا تقوم بالتجسس على ماكنة الصراف الآلي مثلا وعندها يتمكن الجاني من قراءة الارقام التي يضعها العميل داخل ماكنة الصراف الالي[4] أو استخدام الكامرات لالتقاط صور للاشخاص في الاماكن الخاصة أو التقاط صور للوثائق التي تمر في جهاز الاستنساخ[5]، أو التقاط صور لخرائط أو أماكن محظورة أو رسوما[6]، كما يتم السوك الاجرامي بالتقاط المعلومات المعروضة على الشاشة ذهنيا بصورة مباشرة،

(1) د. عبد الفتاح بيومي حجازي، التجارة الالكترونية وحمايتها....، مرجع سابق، ص 83. د. محمد سامي الشوا، مرجع سابق، ص 75 وما بعدها.

(2) د. أيمن عبد الله فكرى، مرجع سابق، ص 658 - 659.

(3) نهلا عبد القادر المومني، مرجع سابق، ص 216. د. عمر ابو الفتوح عبد العظيم الحمامي، مرجع سابق، ص 225، 226. د. خالد ممدوح أبراهيم، فن التحقيق....، مرجع سابق، ص 347.

(4) د. عماد مجدي عبد الملك، مرجع سابق، ص 125.

(5) د. أحمد محمود مصطفى، مرجع سابق، ص125. برهام يوست، ترجمة علي جواد حسين، مرجع سابق، ص334.

(6) د. سعد أبراهيم الاعظمي، جرائم التجسس....، مرجع سابق، ص 212.

أو قيام الفاعل بوضع مكبرات صوت تلتقط المعلومات والبيانات[1]، أو التوصيل على خط تلفوني بوضع مركز تنصت والقيام بتسجيل الاتصالات[2]، وتستخدم أيضا الاقمار الصناعية[3] والتي تقوم بإلتقاط صور عالية الدقة لما يحصل على الارض، إضافة الى التقاط الاتصالات التي تحصل بالاجهزة اللاسلكية أو الهواتف المحمولة[4]. ونشير هنا الى أن الالتقاط المعلوماتي يستهدف إضافة إلى البيانات المتبادلة عبر الشبكات، البيانات المخزونة داخل الحاسب[5].

ومن الجدير بالذكر يرى بعض الفقهاء أن الالتقاط الذهني البصري أو السمعي، لا يتوفر فيه مقومات النشاط المادي الذي له المظهر الخارجي الملموس، وبالتأكيد هذا الرأي لا تأثير له إذ كان هنالك نص يجرم هذه الصورة كالتشريع السعودي[6]والاماراتي[7].

أما التنصت المعلوماتي لغة: يأتي بمعنى تنصت على الحديث، أي تَسَمّع وتكلف النصت، ويقال أنصت، أي استمع وأحسن الاستماع للحديث، إذ تقول أنصت ينصت إنصاتا، وأنصته وأنصت له[8].

(1) د. محمد سامي الشوا، مرجع سابق، ص 74.

(2) د. محمد محمود مكاوي، مرجع سابق، ص 298.

(3) يستخدم في التصوير الجوي مايسمى بالتصوير تحت الحمراء والذي لا يتأثر بسوء الاحوال الجويه والتي تشكل عائق أمام وضوح الصور الملتقطة، كما تسهم هذة الطريقة في قياس عمق البحر في الاماكن الضحلة التي سيجرى فيها أنزال. للمزيد: عبد الفتاح رياض، تصوير ملا تراه العين بالاشعة غير المرئية، دار النهضة العربية، القاهرة، بدون سنة طبع، ص 233.

(4) د. يوسف حسن يوسف، مرجع سابق، ص134. د. حسين المحمدي بوادي، الجاسوسية....، مرجع سابق، ص105.

(5) حمزة بن عفون، مرجع سابق، ص 137.

(6) ينظر: (الفقرة 10 من المادة 1) من نظام مكافحة الجرائم المعلوماتية السعودي.

(7) المادة (1) من مرسوم قانون مكافحة جرائم تقنية المعلومات الاماراتي.

(8) أبراهيم مصطفى وأخرون، المعجم الوسيط، ج2، مرجع سابق، ص 925. الصاحب بن عباد، المحيط في اللغة، ج 2، مرجع سابق، ص 217.

قانونا: حددت (الفقرة 1 من المادة 3) من النظام السعودي لمكافحة الجرائم المعلوماتية مفهوم التنصت المعلوماتي على أنه "التنصت على ماهو مرسل عن طريق الشبكة المعلوماتية أو إحدى أجهزة الحاسب الالي – دون مسوغ نظامي صحيح – ... ".

فقها: يعرف التنصت المعلوماتي بأنه (عملية التقاط المعلومات عبر خطوط الهاتف، والتي تتم مباشرة عند التنصت على المتكلم من خلال وضع مركز تصنت أو مكبرات صوت صغيرة)[1].

وأيضا بأنه(التلصص على ماهو مرسل بواسطة الشبكة المعلوماتية، أو أحد أجهزة الكومبيوتر، دون مسوغ قانوني، أو اعتراضه)[2].

وأيضا (قيام الشخص بالاستماع سرا بأية وسيلة الى حديث بين شخصين أو أكثر أو شخص واحد ولهذا الحديث طابع السرية دون رضاء من تعرض للتنصت)[3].

يقع السلوك الاجرامي لجريمة التنصت المعلوماتي، أما مباشرة وذلك بالدخول للنظام المعلوماتي واستخدامه، وأما بصورة غير مباشرة ويتم ذلك بأفعال استراق السمع أو الاعتراض والالتقاط للمعلومات المنقولة عبر النظام المعلوماتي الالكتروني[4]، من خلال التقاط الموجات الكهرومغناطيسية التي تصدر من الحواسيب حال تشغيله وترجمة هذه البيانات باستخدام هوائي متصل بحاسب آلي خاص لهذا الغرض[5]، أو يقوم الفاعل بوضع مكبرات صوت تقوم بالتقاط البيانات

(1) د. محمد محمود مكاوي، مرجع سابق، ص 254.
(2) د. عبد الفتاح بيومي حجازي، نحو صياغة....، مرجع سابق، ص 62.
(3) د. محمد الشهاوي، مرجع سابق، ص 266.
(4) د. علي جعفر، مرجع سابق، ص 581. عبد الحكيم ذنون يونس يوسف الغوال، مرجع سابق، ص 204.
(5) د. حسام محمد الشنراقي، مرجع سابق، ص 557.

والمعلومات[1]، ويعد السلوك الاجرامي المتقدم أكثر الأفعال شيوعا واسهلها تنفيذا، كما يتم بقيام الفاعل بربط أسلاك بصورة خفية بالحاسب المستهدف للوصول للمعلومات المستهدفة، أو التوصيل على خط تلفوني بوضع مركز تنصت والقيام بتسجيل الاتصالات، أو يتم الوصول الى المعلومات باستخدام الفاعل جهاز حاسب يحتوي على برنامج خاص يقوم بترجمة الارتجاجات والنبضات التي تصتدم بالجدران الاسمنتية وتحويلها إلى عبارات مفهومة[2]، كما يتم التنصت أو الدخول على المكالمات المحددة من قبل المتجسسين باستخدام الكيبل المحوري أو كيبل متعدد الازواج أو الميكروف الراديوي، حيث استطاع المتجسسون من التقاط الاتصالات التي تتم بين مدينتين، كما يتم بإلتقاط الاتصالات الحاسوبية باستخدام نفس الطرق التي تستخدم للتشبيك مع الهاتف بالتقاط المعلومات المتبادلة بين حاسبة طرفية وحاسبة رئيسية[3]، كما يتم السلوك الاجرامي بإلتقاط الاستخبارات الرادارية والاستخبارات الالكترونية والاتصالات التي تحصل بالأجهزة اللاسلكية أو الهواتف المحمولة، ومن ثم القيام بتحليل البيانات الملتقطة من قبل المحطات الأرضية ويتم هذا السلوك من قبل بعض الدول كالولايات المتحدة الأمريكيه مستخدمة في ذلك طائرات التجسس والاقمار الصناعية[4]، حيث قامت وكالة الامن القومي الامريكية بواسطة الحواسيب بالتجسس على كل رسالة أو اتصال هاتفي أو إيميل يتم من قبل الشعب العراقي بأكمله منذ عام 2013 حيث كان قبل

(1) د. عمر ابو الفتوح عبد العظيم الحمامي، مرجع سابق، 221. د. محمد محمود المكاوي، مرجع سابق، ص254.

(2) للمزيد: برهام يوست، ترجمة علي جواد حسين، تكلنوجيا التجسس، ط 1، الدار العربية للموسوعات، بيروت، 1999، ص 287. د. أيمن عبد الحفيظ عبد الحميد سلمان، مرجع سابق، ص 189. نهلا عبد القادر المومني، مرجع سابق، ص 218.

(3) للمزيد: برهام يوست، ترجمة علي جواد حسين، مرجع سابق، ص 326 ومابعدها.

(4) للمزيد: د. يوسف حسن يوسف، مرجع سابق، ص 134. د. حسين المحمدي بوادي، الجاسوسية....، مرجع سابق، ص 105. برهام يوست، ترجمة علي جواد حسين، مرجع نفسه، ص 365 ومابعدها.

ذلك التاريخ يقتصر التجسس على الجماعات المتشددة وتهديدات أخرى[1]، أو قيام الفاعل بأخفاء برامج خبيثة داخل برامج وتطبيقات الحاسب المستهدف ومن خلالها يتم الوصول إلى البيانات عن بعد وتسجيلها أو نقلها دون علم ورضا صاحب النظام المعلوماتي...الخ[2]، أو قيام الفاعل بالتنصت وتسجيل الاحاديث ونقلها بواسطة الهاتف العادي أو المحمول الذي يستخدم شبكة الانترنت بالاتصال وذلك بالتنصت عليه مباشرةً أو بصورة غير مباشرة وذلك بالدخول الى خطوط الهواتف الشخصية[3]، أو التنصت باستخدام فيض التردد الراديوي أو جهاز تنصت إرسالي والذي يعتمد على إلتقاط الصوت وإرساله بشكل موجات لا سلكية وجهاز مسقبل لها يقوم بتضخيم الصوت ليستمع إليه المتجسس وغيرها من البرامج الخاصة بذلك[4] مثل جهاز التنصت الليزري[5].

ومن الجدير بالذكر أنه يشترط لتحقق السلوك الاجرامي في التنصت المعلوماتي، أن يكون الشخص المتنصت قادرا على السمع، وأن يكون الصوت المرسل مسموعاً، وأن يكون الصوت مرسل عن طريق شبكة الانترنت أو إحدى أجهزة الكومبيوتر، ويحصل التنصت دون سبب قانوني[6] كما لم يشترط القانون الفرنسي الجديد أن يحصل التنصت أو التسجيل للحديث في مكان خاص، والذي ذكر السلوك المادي لهذه الجريمة قد يكون باستراق السمع[7] بالاستماع للحديث

---

(1) جيلين جرينوالد، ترجمة بسام شيحا، مرجع سابق، ص 123.

(2) للمزيد: بهاء فهمي الكبيجي، مرجع سابق، ص 49.

(3) د. عبد الفتاح بيومي حجازي، جرائم الكومبيوتر والانترنت في التشريعات العربية، مرجع سابق، ص 120 وما بعدها. وكذلك: مؤلفه، الجرائم المستحدثة...، مرجع سابق، ص 514.

(4) للمزيد: برهام يوست، ترجمة علي جواد حسين، مرجع سابق، ص 271 وما بعدها.

(5) جهاز التنصت الليزري: هو(عبارة عن جهاز تنصت سلبي يقوم بالتقاط اهتزازات محادثات خارج زجاج النافذة الى مسافة نصف ميل ومن ثم ترجمتها الى كلام).

(6) د. خالد ممدوح أبراهيم، فن التحقيق...، مرجع سابق، ص 341.

(7) أستراق السمع تعني: (الاستماع الى الحديث خفيه، وتأتي أختلاس النظر والسمع). محمد بن مكرم بن منظور الافريقي المصري، لسان العرب، ج 10، ط 1، مرجع سابق، ص 155.

دون أن يشعر بذلك صاحب الشأن (خلسة) بواسطة جهاز فهو فعل يتم باستخدام الأذن أو عن طريق جهاز من الأجهزة[1]، أو التسجيل والذي يتم من خلال حفظ الحديث بشكل يمكن الاستماع اليه في وقت لاحق، أو نقل الحديث والذي يتم بواسطة الاجهزة الحديثة وذلك بأرسال الحديث من مكان الى أخر[2].

خلاصة لما تقدم نجد أن السلوك الاجرامي في الاعتراض أو الالتقاط أو التنصت يتشابه إلى حدا ما، حيث يتم السلوك إما بالاتقاط أو الاعتراض أو التنصت على البيانات أو المعلومات أو الاتصالات التي تتم عبر الشبكات المعلوماتية العامة أو الخاصة، أو التي تتم في حاسب واحد أو بين حاسبين في نظام معلوماتي واحد أو بين نظامين مختلفين، مما يجعلنا نؤيد موقف التشريعات الفرنسي والسعودي والاماراتي في تجريم هذه الصور للسلوك الاجرامي في نص واحد، ولم نجد نصاً يجرم هذه الافعال في التشريع الامريكي - بحسب ما اطلعت عليه من مصادر - .

ثانيا: النتيجة الجرمية:

فبالنسبة للإعتراض المعلوماتي لم يجرم التشريع الفرنسي هذه الصورة، وأرى أن فعل الإلتقاط المعلوماتي يتشابه إلى حداً كبير مع الاعتراض المعلوماتي، إذ يترتب على كلاهما الاستماع للحديث أو تسجيله أو نقله، والتي تصدر بصفه سرية أو خاصة دون رضاه صاحب الشأن، ولعدم وجود نص يجرم الإلتقاط المعلوماتي - كما سنبين ذلك في محل الجريمة - لا بد من تدخل المشرع الفرنسي لتجريم إحدى هذه الصور لسد النقص التشريعي.

أما النتيجة الجرمية في التشريع الاماراتي فهي الحصول على المحادثات أو الاتصالات ومواد صوتية أو مرئية شخصية خاصة بالغير، استنادا الى (الفقرة 1 من المادة 21) من مرسوم مكافحة جرائم تقنية المعلومات.

(1) عبد الحكيم ذنون يونس يوسف، مرجع سابق، ص 205.
(2) د. طارق صديق رشيدكه ردى، مرجع سابق، ص 219.

في حين لم يحدد النظام السعودي نتيجة معينة في نص (الفقرة 1 من المادة 3) من نظام مكافحة الجرائم المعلوماتية حيث جاء عاما، " التنصت على ماهو مرسل عن طريق الشبكة المعلوماتية، أو إحدى أجهزة الحاسب الآلي، ... أو التقاطه أو اعتراضه ". وعليه فهو يشمل جميع ما يرسل عبر الشبكة المعلوماتية أو أجهزة الحاسب، من بيانات أو معلومات أو صور أو إتصالات....الخ.

وكذلك لم يحدد مشروع قانون الجرائم المعلوماتية العراقي نتيجة معينة حيث نصت (الفقرة ز من المادة 14) على أن " التقط أو اعترض.... ماهو مرسل عن طريق أحد أجهزة الحاسوب أو شبكة المعلومات لاستخدامها... ".

في حين يتطلب السلوك الاجرامي للاعتراض نتيجة جرمية، كنتيجة مباشرة لعملية اعتراض الموجات الكهربائية، وذلك بالوصول إلى المعلومات المحفوظة داخل النظام المعلوماتي للغير، كالحصول على أرقام بطاقات الائتمان مثلا[(1)]، ويرى بعض الفقهاء باتفاق الاعتراض مع الدخول غير المشروع، في أن كلا منها يؤدي إلى نتيجة واحدة هو الوصول إلى معلومات غير مصرح للفاعل الوصول إليها، ففي الأولى يتم الوصول بصورة غير مباشرة أما الثانية فيتم مباشرةً، إلا أنهما يختلفان في كون جريمة الدخول غير المشروع تتطلب تشغيل النظام المعلوماتي ومن ثم الدخول إليه، أما جريمة الاعتراض فإنه يفترض أن الحاسب الآلي قد بدء تشغيله بالفعل[(2)].

ويمكن أن نضيف فرقا آخر بينهما يتمثل في أن جريمة الدخول غير المشروع، قد ترتكب من شخص له صفة كالموظف أو المخول بالدخول للنظام المعلوماتي، فيتجاوز السلطة الممنوحه له، أما الاعتراض أو الالتقاط أو التنصت فإن أغلب

(1) د. حسين بن محمد الغافري، مرجع سابق، ص 284.

(2) د. احمد محمود مصطفى، مرجع سابق، ص 257 وما بعدها.

صورها أنها ترتكب من أشخاص غير مخولين وإن كان بالإمكان أن يكون ارتكابها تنفيذا للقانون.

أما الالتقاط المعلوماتي فإن النتيجة الجرمية في التشريع الفرنسي هي الحصول على صورة شخص أو تسجيلها[1] أو نقلها والتي تلتقط في مكان خاص للمجني عليه دون رضاه، استنادا إلى نص (الفقرة 1 من المادة 226)، ومن الجدير بالذكر لا يتطلب في هذه الجريمة تحقق نتيجة إجرامية دائما بل يكفي مجرد تحقق السلوك[2] كما في الالتقاط الذهني.

في حين أن النتيجة الجرمية في التشريع الاماراتي هي إلتقاط صور للغير أو إعداد صور ألكترونية أو نقلها أو كشفها أو نسخها أو الإحتفاظ بها، استنادا الى (الفقرة 2 من المادة 21) من مرسوم مكافحة الجرائم التقنية.

أما النظام السعودي لمكافحة الجرائم المعلوماتية فإنه لم يحدد نتيجة معينة، وذلك في نص (الفقرة 1 من المادة 3)، حيث جاء النص عاما.

وكذلك جاء مشروع الجرائم المعلوماتية العراقي خالي من تحديد أي نتيجة في نص (الفقرة ز من المادة 14).

أما التنصت المعلوماتي فإنه النتيجة الجرمية في التشريع الفرنسي هي الاستماع للأحاديث والتي تصدر بصفة سرية أو خاصة دون رضا صاحب الشأن، استنادا إلى (الفقرة 2 من المادة 226)

في حين أن النتيجة الجرمية في التشريع الإماراتي هي محادثات أو إتصالات ومواد صوتية أو مرئية خاصة بالغير استنادا الى (الفقرة 1 من المادة 21)، ومن

(1) يقصد بالتسجيل: (حفظ صورة الشخص على مادة معدة لهذا الغرض بأية وسيلة كانت لمشاهدتها لاحقا أو لأذاعتها، مثل رسم صورة شخص يوجد في مكان خاص). ينظر: د. طارق صديق رشيدكه ردى، مرجع سابق، ص224.

(2) د. نائلة عادل محمد فريد قورة، مرجع سابق، ص 341.

الجدير بالذكر أن المشرع الاماراتي استبدل لفظ التنصت بلفظ استراق السمع، حيث كان التشريع القديم الخاص بجرائم التقنية لعام 2006 يستخدمها.

ولم يحدد النظام السعودي في (الفقرة 1 من المادة 3) من قانون مكافحة الجرائم المعلوماتية، نتيجة معينة تترتب على فعل التنصت.

وعلى نفس المسار جاء مشروع الجرائم المعلوماتية العراقي في (الفقرة ز من المادة 14).

ثالثا: العلاقة السببية:

- كما سبق القول - أن العلاقة السببية هي امكانية إسناد نتيجة إلى فعل وربطها برباط وثيق، أي ارتباط السبب بالمسبب ومن ثم فهي عنصر لازم في جميع الجرائم عمدية كانت أم غير عمدية، وحتى يسأل الفاعل عن النتيجة الجرمية لابد أن تكون النتيجة المتحققة هي نتيجة لسلوكه الإجرامي، أما إذا لم تكن كذلك فلا يسأل عنها حتما، فالفاعل في هذه الجريمة يريد الفعل ويريد النتيجة[1]، فبالنسبة الى جريمتي الاعتراض و التنصت تعد - كما سبق بيانه - من الجرائم المادية والتي تتطلب نتيجة معينة، أما جريمة الالتقاط فإنها تتحقق في بعض صورها بمجرد صدور الفعل كما هو في حالة الالتقاط الذهني حيث أن الجريمة تقع تامة بمجرد النظر إلى المعلومات المعروضة على الشاشة مثلا والاستحواذ عليها ذهنيا، والبعض الآخر من صور الالتقاط هي من الجرائم المادية حيث تتطلب علاقة سببيةً بين التقاط الصورة و نشرها مثلا.

(1) د. عبد الفتاح بيومي حجازي، جرائم الكومبيوتر والانترنت في التشريعات العربية، مرجع سابق، ص 121.

الفرع الثاني

الركن المعنوي

يكفي القصد الجرمي العام في هذه الجرائم، وهو علم الجاني بأنه يعترض أو يتنصت على المكالمات والأحاديث الشخصية وتسجيلها ونقلها، أو لبيانات ليس من حقه الاطلاع عليها، حيث يعلم الجاني بأن فعله يشكل اختراقاً لسرية ماهو مرسل عن طريق الشبكة المعلوماتية أو إحدى أجهزة الحاسوب، و أنه ليس له الحق بالتنصت أو الالتقاط أو اعتراض على هذه المراسلات أو الاتصالات الالكترونية، ومع ذلك تتجه ارادته للقيام بذلك، فإن كان يعتقد خطأ أن الاستماع إلى هذه المراسلات متاح للجميع أو كان يعتقد خطأ أن من حقه الاستماع لها، أو أن الاطراف المسؤولة عن النظام المعلوماتي قد صرحة له مراقبة الاتصالات، كما في حالة من صدر له الاذن بالتنصت على مواد معينة لملاحقة المتهم وإيقاف العمل بالإذن دون أن يعلم بذلك، أو كان دخوله الى نطاق الاتصالات صدفة وتوقف نشاطه عند هذا الحد، فهنا ينتفي عنصر العلم وبالتالي لا قيام للركن المعنوي أو الجريمة [1]، فالجاني يعلم عند قيامه بالفعل أنه يخالف أحكام القانون ومع ذلك تتجه إرادته إلى الفعل قابلا بالنتيجة المتحققة[2]، كاستراق السمع مثلا على المعلومات المنقولة عبر شبكات الاتصالات[3]، أما إذا كان مكرها من قبل غيره بوسائل الاكراه المادي أو المعنوي فلا يقوم الركن المعنوي وبالتالي لا قيام للجريمة[4]، بمعنى لا تقوم

(1) د. خالد ممدوح أبراهيم، فن التحقيق...، مرجع سابق، ص 341 - 342. د. عبد الفتاح بيومي حجازي، نحو صياغة....، مرجع سابق، ص 177. بلال أمين زين الدين، مرجع سابق، ص310.

(2) د. عبد الفتاح بيومي حجازي، جرائم الكومبيوتر والانترنت في التشريعات العربية، مرجع سابق، ص 121.

(3) د. أيمن عبد الله فكري، مرجع سابق، ص 648.

(4) بلال أمين زين الدين، مرجع سابق، ص 310. د. أحمد محمود مصطفى، مرجع سابق، ص 257.

جريمة الاعتراض أو الالتقاط أو التنصت المعلوماتي حتى وإن توافر الركن المعنوي للجريمة في حالتين الاولى: هي عدم توفر القصد الجرمي والحالة الثانية: إذا كان ذلك التنصت أو الالتقاط أو الاعتراض تنفيذا للقانون[1]. وتستهدف الأفعال المتقدم ذكرها المحادثات أو المراسلات الشخصية وتسجيلها أو إلتقاط الرسائل سواء تعلقت بالحياة الخاصة أو غيرها[2]، و بالتأكيد لا يقف محل الجريمة عند هذا الحد فهي تشمل التنصت أو الالتقاط أو الاعتراض للمراسلات التي تتعلق بنظم المعالجة الحكومية أو مراسلات القطاع الخاص وكذلك البيانات أو المعلومات...الخ،[3]، وكذلك الصور الشخصية التي تلتقط للشخص في مكان خاص دون رضاه[4].

(1) المادة (1/9/432) من قانون العقوبات الفرنسي الجديد.

(2) د. عبد الفتاح بيومي حجازي، جرائم الكومبيوتر والانترنت في التشريعات العربية، مرجع سابق، ص 120 وما بعدها.

(3) د. عبد الفتاح بيومي حجازي، نحو صياغة...، مرجع سابق، ص 171 وما بعدها.

(4) المادة (226) من قانون العقوبات الفرنسي الجديد.

المطلب الثاني

الركن المفترض وعقوبة الجريمة

نتناول في هذا المطلب محل جريمة الاعتراض أو الالتقاط أو التنصت المعلوماتي، بفرعين وعلى النحو الآتي:

- **الفرع الاول:** محل الجريمة.
- **الفرع الثاني:** عقوبة الجريمة.

الفرع الاول

محل الجريمة

يختلف محل الجريمة باختلاف التشريعات التي جرمت هذه الافعال، ففي التشريع الفرنسي محل جريمة التنصت هو الاحاديث الخاصة التي تصدر عن شخص بصفه سرية أو خاصة دون رضاه، أما محل جريمة الالتقاط فهو صورة شخص يوجد في مكان خاص دون رضاه، استنادا الى (الفقرة 1 من المادة 226)، ومن الجدير بالذكر حاول بعض من الفقهاء الفرنسيين سد النقص التشريعي المتعلق بتجريم فعل إلتقاط البيانات المعلوماتية وذلك بتطبيق نص (الفقرة 1 من المادة 226) على فعل التقاط المعلوماتي للبيانات، إلا أن محاولتهم لم تنجح لأن المادة المذكورة تجرم الالتقاط للأقوال والصور الخاصة، و أن الالتقاط بصورة عامة قد ينصب على محرارات أو أرقام..الخ، وهي ليست أقوالا أو صوراً[1].

أما الاعتراض فلم يتناوله المشرع الفرنسي - حسبما اطلعت عليه - مما يستدعي تدخل المشرع الفرنسي بادراج نص يجرم الاعتراض أو الالتقاط للبيانات أو المعلومات أو الاتصالات وغيرها.

في حين أن محل جريمة الاعتراض أو الالتقاط أو التنصت في النظام السعودي هو الشبكة المعلوماتية، أو إحدى أجهزة الحاسب الآلي، استنادا الى (الفقرة 1 من المادة 3) من نظام مكافحة الجرائم المعلوماتية. وهنا قد ضيق النظام السعودي من محل الجريمة بسبب تحديده، ولم تكن هنالك صياغة مرنه كما فعل المشرع الاماراتي كما سنبين.

(1) د. سمية عكور، مرجع سابق، ص 7.

وفي التشريع الاماراتي فإن محل الجريمة هو الشبكة المعلوماتية أو نظام معلوماتي ألكتروني، أو إحدى وسائل تقنية المعلومات، استنادا إلى (الفقرة 1 من المادة 21) من مرسوم بقانون مكافحة جرائم تقنية المعلومات، ما يلاحظ على التشريع الاماراتي الصياغة المرنة حيث جعل الباب مفتوحا عندما ذكر عبارة " أو إحدى وسائل تقنية المعلومات" وهو أمر مستحسن.

أما محل جريمة الاعتراض أو الالتقاط في مشروع قانون الجرائم المعلوماتية العراقي فهو أحد أجهزة الحاسوب أو شبكة المعلومات، استنادا الى (الفقرة ز من المادة 14). ولم يجرم المشروع العراقي في مشروع قانون الجرائم المعلوماتية التنصت المعلوماتي أو فعل الاستراق.

نخلص مما تقدم أن محل الجريمة في الاعتراض أو الالتقاط أو التنصت (استراق السمع) المعلوماتي، هو الاحاديث أو الصور الخاصة، أو الشبكة المعلوماتية، أو نظام معلوماتي الكتروني، أو إحدى أجهزة الحاسب، أو أحدى وسائل التقنية.

الفرع الثاني

عقوبة الجريمة

بالنسبة للعقوبة الأصلية عاقب المشرع الفرنسي على جريمة التنصت و جريمة الالتقاط، بالحبس وبالغرامة التي لا تزيد على ثلاثمائة الف فرنك في (الفقرة 1 من المادة 226) من قانون العقوبات النافذ.

في حين عاقب النظام السعودي على جريمة التنصت أو الالتقاط أو الاعتراض، بالسجن مدة لاتزيد عن سنة وبغرامة لا تزيد على خمسمائة الف ريال، أو بإحدى هاتين العقوبتين في نص (الفقرة 1 من المادة 3) من نظام مكافحة الجرائم المعلوماتية.

أما المشرع الاماراتي فقد عاقب على جريمة استراق السمع أو الالتقاط أو الاعتراض، بالحبس مدة لا تقل عن ستة أشهر والغرامة التي لاتقل عن مائة وخمسين ألف درهم ولا تتجاوز خمسمائة ألف درهم أو بإحدى هاتين العقوبتين كل من استخدم شبكة معلوماتية أو نظام معلوماتي الكتروني، أو إحدى وسائل تقنية المعلومات، في الاعتداء على خصوصية شخص في غير الاحوال المصرح بها قانونا بأحدى الطرق التالية: 1 - استراق السمع أو اعتراض أو تسجيل أو نقل أو بث أو افشاء محادثات أو اتصالات ومواد صوتية أو مرئية. 2 - التقاط صور الغير أو إعداد صور الكترونية أو نقلها أو كشفها أو نسخها أو الاحتفاظ بها. 3 - نشر أخبار أو صور الكترونية أو صور فوتوغرافية أو مشاهد أو تعليقات أو بيانات أو معلومات ولو كانت صحيحة وحقيقية. كما يعاقب بالحبس مدة لا تقل عن سنة واحدة والغرامة التي لا تقل عن مائتين وخمسين الف درهم ولا تتجاوز خمسمائة الف درهم أو بإحدى هاتين العقوبتين، كل من استخدم نظام معلوماتي الكتروني،

أو إحدى وسائل تقنية المعلومات، لإجراء أي تعديل أو معالجة على تسجيل أو صورة أو مشهد، بقصد التشهير أو الاساءة إلى شخص آخر، أو الإعتداء على خصوصيته أو إنتهاكها"، استنادا للمادة (21) من مرسوم مكافحة جرائم تقنية المعلومات.

- كما سبق أن ذكرنا - أن مشروع قانون الجرائم المعلوماتية العراقي لعام 2012 جاء خاليا من نصوص عقابية.

وفيما يتعلق بالعقوبات الفرعية فأننا نحيل الى ما سبق ذكره في هذا الصدد في جريمة الدخول غير المشروع [1] تجنبا للتكرار.

(1) العقوبات الفرعية ينظر ص 138 ومابعدها من الرسالة.

الخاتمة

بعد أن انتهينا بحمد الله وتوفيقه من دراسة موضوع (جريمة التجسس المعلوماتي/ دراسة مقارنة) توصلنا الى عدد من النتائج والتوصيات نورد أهمها.

أولا: النتائج:

1.لم يكن هنالك تعريف جامع مانع للجريمة المعلوماتية على الصعيدين الفقهي والقانوني، بل توجد تعريفات تبرز جانباً معيناً كالمعرفة بالتقنية أو جانب الربح والخسارة...الخ، الا أني تمكنت من تعريف الجريمة المعلوماتية (كل فعل أو امتناع، غير مصرح به يرتكب باستخدام تقنية المعلومات، يقع على الانظمة المعلوماتية أو المواقع الالكترونية أو الشبكات أو أيا من الوسائل التقنية، يترتب عليه ضرر، سواء حقق الجاني مكسبا أم لا).

2.تتميز الجريمة المعلوماتية بصعوبة الاثبات، ومع ذلك بالامكان إثباتها من خلال استخدام بعض البرامج التي تتمكن من إيجاد أدلة الجريمة المعلوماتية حتى في حال إتلاف القرص الصلب، كما تتمكن هذه البرامج من متابعة مرتكبي الجريمة والوصول اليهم.

3.أوضحت الدراسة أن هنالك مخاطراً طبيعية وعامة لها أضرار على الانظمة المعلوماتية أقوى بكثير من البرامج الالكترونية الضارة، كما أن البرامج الضارة تختلف في تأثيرها وكيفية الإصابة بها، حيث يظهر البعض منها على أنها برامج صالحة تؤدي عملا معيناً، وهي في حقيقتها برامج تجسسية تبدء بعد فترة من الزمن بالعمل الضار كبرنامج حصان طروادة مثلا.

4.إن أغلب برامج النظام المعلوماتي تحوي على ثغرات عند صناعتها، لأسباب متعددة قد تكون لحداثة البرنامج أو تعمد صانعو هذة البرامج وضعها لأغراض التجسس أو السرقة أو غير ذلك.

5.بينت الدراسة أن الأمن المعلوماتي لا يقتصر على النظم المعلوماتية، بل يشمل أمن البنايات والعاملين فيها والحواسيب...الخ، و أن هنالك برامج كجدران الحماية وبرامج بيولوجية يمكن الاستعانة بها، للحفاظ على أمن النظم المعلوماتية وما تحوية من بيانات أو المعلومات أو البرامج...الخ.

6.لم تعرف أغلب التشريعات التجسس التقليدي أو المعلوماتي، كما أنها لم تطلق عليه لفظ التجسس، بل الدخول غير المشروع أو الاعتراض أوالالتقاط أو التنصت المعلوماتي كما أن جريمة إفشاء الإسرار ماهية إلا صورة من صور التجسس إلا أنها ترتكب من شخص له صفة في الغالب، وقد تمكنت من وضع تعريف للتجسس المعلوماتي على أنه (الدخول غير المصرح به أو تجاوز التصريح الممنوح، إلى نظام معلوماتي أو موقعاً الكتروني أو شبكة معلوماتية، أو أية وسيلة تقنية أخرى، باستخدام الشبكة المعلوماتية أو الحاسب الآلي أو إحدى الوسائل التقنية، لانتهاك سرية البيانات الحكومية أو الخاصة، بالاطلاع عليها أو نسخها أو نشرها أو إذاعتها أو إفشائها أو كشفها أو تسليمها الى الغير(دولة، شركات، فرد..الخ)، بمقابل أو بدون مقابل).

7.أظهرت الدراسة أن جريمة الدخول غير المشروع من الجرائم الشكلية التي تتحقق بمجرد الدخول للنظام المعلوماتي أو موقع ألكتروني أو شبكة معلوماتية أو أي تقنية أخرى، في حين أن جريمة الاعتراض أو التنصت المعلوماتي من الجرائم المادية أما الالتقاط المعلوماتي فهي شكلية في بعض صورها كما في صورة المشاهدة والالتقاط الذهني.

ثانيا: التوصيات:

1.أدعو الى توحيد المصطلحات المستخدمة للدلالة على التجسس على المستوى الدولي والوطني، وفضلت استخدام مفردة التجسس وليس تحت عناوين مغايرة كالدخول غير المشروع أو التنصت أو الالتقاط أو الاعتراض...الخ.

نوصي المشرع العراقي بتعديل نص المادة (40) من الدستور العراقي لعام 2005 والتي منعت الاعتداء على المراسلات البريدية والبرقية والهواتف دون ذكر النظم المعلوماتية أو الشبكات..الخ، كما منعت الاعتداء على الاتصالات وغيرها، لضرورة قانونية وأمنية، ما يلاحظ على النص أنه منع الاعتداء على المراسلات البريدية والبرقية والهواتف دون ذكر النظم المعلوماتية أو الشبكات المعلوماتية...الخ، كما منع الاعتداء على الاتصالات وغيرها، لضرورة قانونية وأمنية، والادق أستخدام عبارة لضرورة قانونية أو أمنية للتخيير بينهما، ونقترح تعديل النص على النحو الاتي "لا يجوز الاعتداء على الانظمة المعلوماتية أو الشبكات المعلوماتية أو المواقع الالكترونية أو المراسلات البريدية أو البرقية أو الهاتفية أو غيرها من وسائل التقنية، بالتنصت أو المراقبة أو الكشف أو الافشاء أو الاعتراض أو الالتقاط أو الدخول غير المشروع أو غير ذلك، الا لضرورة قانونية أو أمنية وبقرار قضائي".

2.أن نص المادة (3) من مشروع قانون الجرائم المعلوماتية العراقي لعام 2012 وردت فيه عبارة " تقنية المعلومات" فقط، و الافضل إيراد عبارة " النظم المعلوماتية أو الشبكة المعلوماتية أو المواقع الالكترونية أو غيرها من الوسائل التقنية "، يضاف الى ذلك إشتراط النص لتحقق الجريمة أن يكون هنالك اعتداء على " البيانات المحفوظة والانظمة الالكترونية وشبكات الاتصال "، والافضل استخدام عبارة " أو" بدل من عبارة " و" لأن الاعتداء على أحدها يكفي لقيام جريمة، كما أن عبارة " والحاق الضرر بالمشتركين والمستفيدين"، لم تكن دقيقة لأن جريمة التجسس هي من جرائم الخطر وتجرم حتى لو لم يكن هنالك ضرر، لتوفر الحماية للبيانات أو المعلومات أو غيرها من أي انتهاك لسريتها، كما ورد في النص عبارة " الحصول على معلومات حكومية سرية" ماذا يراد بها هل هي ظرف مشدد أم ماذا؟، ومن الجدير بالاشارة أن مشروع قانون الجرائم المعلوماتية لعام 2012 قد خلا من أحكام عقابية حيث وردت (الاحكام العقابية بحاجة الى دراسة من القانونيين) وبالتالي يكون النص المقترح " 1 - يعاقب بالسجن والغرامة التي لا تزيد عن عشرة ملايين أو باحدى هاتين العقوبتين، كل من دخل أو اتصل أو اعترض دون تصريح أو تجاوز التصريح الممنوح له، في موقع الكتروني أو نظام معلوماتي أو شبكة معلوماتية أو أية وسيلة تقنية أخرى، في كل أو جزء منها، باستخدام وسائل التقنية، وتكون العقوبة السجن مدة لا تقل عن سبع سنوات والغرامة التي لاتقل عن عشرة ملايين أو بإحدى هاتين العقوبتين، إذا ترتب عن ذلك محو أو تعديل أو تشوية أو نسخ أو نقل أو إفشاء أو نشر أو تسجيل أو تدمير للبيانات أو البرامج المحفوظة أو للأجهزة أو الأنظمة الالكترونية أو شبكات الاتصال أو غير ذلك، سواء كانت تابعة للمؤسسات الاقتصادية أو التجارية أو المالية أو الصناعية أو العلمية أو المشتركين أو المستفيدين. 2 - تكون العقوبة السجن المؤبد أو المؤقت و الغرامة إذا حصل الجاني على بيانات أو معلومات حكومية سرية أو مايعتبر كذلك".

3.ورد في المادة (4) من مشروع قانون الجرائم المعلوماتية العراقي لفظ " المتعمد" وهي زائدة فالاعتراض لا يقع إلا عمدا، كما وردت عبارة " الوسائل الفنية" والأفضل استخدام عبارة "الوسائل التقنية" لأنها أشمل و أدق، كما أن النص لم يوضح هل كل أعتراض مجرم، وما هو الوضع القانوني للإعتراض الذي يقع تنفيذا للقانون، لذلك اقترحنا إعادة الصياغة على النحو الاتي " يعاقب بالحبس والغرامة التي لا تقل عن مليون دينار أو بإحدى هاتين العقوبتين، كل من اعترض أو التقط أو تنصت بدون تصريح أو تجاوز التصريح الممنوح له، لخط سير البيانات أو المعلومات أو الاتصالات أو الصور أو غير ذلك، وتكون العقوبة هي الحبس لمدة لا تقل عن ثلاث سنوات و الغرامة التي لا تقل عن ثلاثة ملايين أو إحدى هاتين العقوبتين، إذا ترتب عن ذلك إفشاء أو كشف أو إذاعة أو نقل أو تسجيل أو نشر لتلك البيانات أو المعلومات أو الاتصالات أو الصور أو غير ذلك ".

4.وفيما يتعلق بنص المادة (5) من مشروع قانون الجرائم المعلوماتية العراقي، حيث جاء النص مبتورا لم يتطرق الى السلوك الاجرامي كأن يقال "كل من دخل أو اعترض"، كما لم يبين الى أي شئ يتم الدخول إليه واعتراضه، هل هي الأنظمة المعلوماتية أو الشبكات...الخ، كما انتقد ورود عبارة "الدخول واعتراض الشبكات الحرجة للدولة" وذلك لأن الدخول يختلف عن الاعتراض وكلاهما مجرم ولايشترط تحققهما معا من أجل تجريم الفعل، كما أن عبارة الشبكات الحرجة، عبارة غامضة تثير اللبس والافضل استخدام عبارة " الدخول أو اعتراض الشبكات أو المواقع الالكترونية أو النظم المعلوماتية أو أية من وسائل التقنية الحكومية أو المستخدمة من قبل الحكومة أو تؤدي عملا لخدمة الحكومة"، كما يأخذ على النص أشتراطه قصداً خاصا هو " المساس بأمن الدولة الداخلي أو

الخارجي أو تعريضها للخطر أو استخدامه عمدا أجهزة الحاسوب وبرامجه أو أنظمته أو شبكة المعلومات التابعة للجهات الامنية أو العسكرية أو الاستخبارية بقصد الاضرار بها أو النسخ منها أو بقصد إرسال محتواها لجهة معادية أو الاستفادة منها في جرائم ضد أمن الدولة الداخلي أو الخارجي، أو تسهيل إخفاء معالم تلك الجرائم أو تغطيتها "، في حين أن جريمة التجسس يكفي لتحققها القصد الجرمي العام، كما أن عبارة " الجهات الاستخباراتية " زائدة لا مبرر لذكرها لأنها إحدى الأجهزة الأمنية، والصياغة المقترحة هي " 1 - يعاقب بالسجن والغرامة، كل من اعترض أو التقط أو تنصت أو دخل بغير تصريح أو تجاوز التصريح الممنوح له، إلى موقع الكتروني، أو نظام معلوماتي ألكتروني، أو شبكة معلوماتية، أو أيا من الوسائل التقنية، باستخدام وسائل تقنية المعلومات. 2 - وتكون العقوبة هي السجن مدة لا تقل عن عشرة سنوات والغرامة، إذا نتج عن ذلك إتلاف أو عيب أو إعاقه أو اطلاع أو نسخ أو تسجل أو إذاعة أو كشف أو إفشاء أو نشر أو تسليم، للبيانات أو المعلومات أو الأنظمة الالكترونية أو المواقع الالكترونية أو الشبكات، الحكومية أو ما يعتبر كذلك ".

5.وردت في (الفقرة د من المادة 7) اشتراطها القصد الجرمي الخاص حيث يكفي القصد الجرمي العام، ونقترح تعديلها على النحو الآتي " يعاقب بالحبس والغرامة التي لا تقل عن ثلاثة ملايين دينار أو بإحدى هاتين العقوبتين، كل من علم بحكم عمله ببيانات التوقيع الالكتروني أو الرسائل الالكترونية أو المعلومات فأفشاها للغير أو قام بنشرها أو نسخها أو تسجيلها أو حذفها أو أتلافها أو أستخدامها في غير الغرض الذي قدمت من أجله"

6.وجرمت المادة (14) من مشروع قانون الجرائم المعلوماتية العراقي، الاعتداء على سرية الحياة الخاصة وذلك في الفقرات (د - ز)، وقد جاءت

صياغة هذه الفقرات ركيكة ونقترح الصياغة الاتية " يعاقب بالحبس مدة لا تقل عن ستة أشهر والغرامة التي لا تقل عن مليون دينار ولا تزيد عن سبعة ملايين أو بإحدى هاتين العقوبتين، كل من استخدم شبكة معلوماتية، أو نظام معلوماتي ألكتروني، أو إحدى وسائل تقنية المعلومات، في الاعتداء على خصوصية شخص في غير الاحوال المصرح بها قانونا بأحدى الافعال الاتية: د - كل من دخل أو أتصل أو أعترض، النظام المعلوماتي أو موقع الكتروني أو شبكة معلوماتية أو أية من الوسائل التقنية، دون تصريح أو بتجاوز التصريح الممنوح له، وترتب على ذلك أعتداء على الحياة الخاصة للشخص نفسه أو لعائلته. ه - استراق السمع أو اعتراض أو تسجيل أو نقل أو بث أو إفشاء محادثات أو اتصالات ومواد صوتية أو مرئية أو استخدام حاسب عائدٍ للغير بصورة مباشرة أو غير مباشرة. و - إلتقاط صور للغير أو اعداد صور الكترونية أو نقلها أو كشفها أو حذفها أو تعيبها أو إعادة نشرها أو نسخها أو الاحتفاظ بها. ز - التقط أو اعترض أو نشر أخباراً أو صوراً الكترونية أو صوراً فوتوغرافية أو مشاهد أو تعليقات أو بيانات أو معلومات ولو كانت صحيحة وحقيقية دون تصريح أو تجاوز التصريح الممنوح له. كما يعاقب بالحبس مدة لا تقل عن سنة واحدة والغرامة التي لا تقل ثلاثة ملايين دينار ولا تزيد عن عشرة ملايين دينار أو بإحدى هاتين العقوبتين، كل من استخدم نظام معوماتي الكتروني، أو إحدى وسائل تقنية المعلومات، لإجراء أي تعديل أو معالجة على تسجيل أو صورة أو مشهد، بقصد التشهير أو الإساءة إلى شخص آخر، أو الاعتداء على خصوصيته أو انتهاكها ".

7.أوصي المشرع العراقي بإدراج نص في مشروع قانون الجرائم المعلوماتية يوفر نوعا من الحماية للنظم المعلوماتية أو التقنية و يكون النص بالصيغة الآتية " يستخدم داخل المؤسسات الحكومية وشبه الحكومية، نظم معلوماتية

وبرامج حماية للبيانات أو المعلومات وغيرها من الوسائل التقنية مصنعة في العراق، أو من مناشئ رصينة تخضع لإشراف كادر من المهندسين العراقيين المختصين لبيان مدى الأمان الذي توفره هذه النظم المعلوماتية أو التقنية للبيانات أو المعلومات المخزنه في داخلها ".

8.ولعدم تضمن مشروع قانون الجرائم المعلوماتية العراقي للعقوبات التبعية والتكميلية والتدابير الاحترازية نقترح النص الاتي "1 - مع عدم الاخلال بحقوق الغير حسن النية يحكم في جميع الاحوال بمصادرة الاجهزة أو البرامج أو الوسائل المستخدمة في ارتكاب أي من الجرائم المعلوماتية أو الاموال المتحصلة منها، ومحو أو أعدام البيانات أو المعلومات، كما يحكم بغلق المحل أو الموقع الذي يرتكب فيه أي من هذه الجرائم، أغلاقاً كلياً أو المدة التي تقدرها المحكمة. 2 - تصدر المحكمة قراراً يقضي بإبعاد الاجنبي الذي يرتكب احدى الجرائم المعلوماتية خارج العراق، وذلك بعد تنفيذ العقوبة المحكوم بها. 3 - يجوز للمحكمة أن تصدر قرار يقضي بوضع المحكوم عليه تحت الإشراف أو المراقبة أو الحرمان، من استخدام الشبكة المعلوماتية أو نظام معلوماتي تقني أو أي وسيلة تقنية أخرى، أو وضعه في مأوى علاجي أو مركز تأهيل للمدة التي تحددها المحكمة ".

9.في حال عدم إقرار مشروع قانون الجرائم المعلوماتية نقترح تعديل نص المادة (328) من قانون العقوبات العراقي ويكون النص المقترح " يعاقب بالسجن مدة لا تزيد على سبع سنوات أو بالحبس كل من اعتدى على الانظمة المعلوماتية أو الشبكات أو المواقع الالكترونية أو البريد أو البرق أو التلفون أو غيرها من الوسائل التقنية، أو قام بفتح أو إفشاء أو نسخ أو نشر أو إتلاف أو إخفاء لبيانات أو معلومات أو صور أو غير ذلك، إذ ارتكبت تلك الافعال من موظف أو مكلف بخدمة عامة عد ذلك ظرفا مشددا ".

10.تعديل نص المادة (438) من قانون العقوبات العراقي " يعاقب بالحبس مدة لاتزيد على ثلاثة سنوات وبغرامة لاتزيد على عشرة ملايين أو بإحدى هاتين العقوبتين، كل من نشر أو نقل أو كشف أو نسخ أو سجل أو بث أو أفشى أو احتفظ أو التقط أو أعترض أو تنصت أو غير ذلك، لأخبارٍ أو صورٍ للغير أو مشاهد أو تعليقات أو محادثات أو اتصالات ومواد صوتية أو مرئية أو بيانات أو معلومات ولو كانت صحيحة وحقيقية، أو إعداد صور الكترونية أو فوتوغرافية تتصل بحرمة الحياة الخاصة أو العائلية للأفراد، سواء باستخدم نظام معلوماتي ألكتروني أو شبكة معلوماتية، أو إحدى وسائل تقنية المعلومات، أو غير ذلك".

11. تعديل نص المادة (363) من قانون العقوبات العراقي على أن " يعاقب بالحبس من تسبب عمدا في ازعاج أو انتهاك سرية البيانات أو المعلومات أو النظام المعلوماتي أو الموقع الالكتروني أو شبكة المعلومات أو غيرها من وسائل التقنية التابعة للغير ".

المصادر

- **القرآن الكريم.**
- **أولا: المصادر باللغة العربية:**

أ - كتب اللغة والمعاجم:

1. إبراهيم مصطفى وآخرون، المعجم الوسيط، ج1، ط 2، دار الدعوة، استانبول، 1989.
2. د. أحمد مختار عمر، معجم اللغة العربية المعاصرة، ط 1، عالم الكتاب، القاهرة، 2008.
3. إسماعيل بن حماد الجوهري، تحقيق أحمد عبد الغفور عطار، تاج اللغة وصحاح العربية، ج 1، دار الكتاب العربي، القاهرة، دون سنة نشر.
4. الحسن بن محمد بن الحسن الصاغاني، العباب الزاخر واللباب الفاخر، تحقيق محمد حسن ال ياسين، ج 1، دار الرشيد للنشر، بغداد، 1981.

5. الخليل بن احمد بن عمرو الفراهيدي، تحقيق مهدي المخزومي و إبراهيم السامرائي، معجم كتاب العين، ج 1، دار الحرية للطباعة، بيروت، 1985.

6. الصاحب بن عباد، المحيط في اللغة، ج2، مطبعة المعارف، بغداد، 1975.

7. بكر بن عبد الله أبو زيد، معجم المناهي اللفظية ويليه فوائد في الالفاظ، ج21، ط3، دار العاصمة، الرياض، 1996.

8. حارث سليمان الفاروقي، المعجم القانوني عربي - أنكليزي، ج4، مكتبة لبنان، بيروت، 1972.

9. خياط يوسف، لسان العرب المحيط، دار لسان العرب، بيروت، 1960.

10. عبد الرحمن حسن حبنكة الميداني، البلاغة العربية أساسها وعلومها وفنونها، ج1، ط1، دار القلم، دمشق، 1996.

11. محمد بن ابي بكر عبد القادر الرازي، مختار الصحاح، مكتبة لبنان، بيروت، 1986، 2010.

12. محمد بن عبد القادر الرازي، مختار الصحاح، دار الرسالة، الكويت، 1982.

13. محمد بن مكرم بن منظور الافريقي المصري، لسان العرب، ج 6، دار صادر، بيروت، 1997.

14. محمد بن يعقوب الفيروز آبادي، تحقيق محمد نعيم العرقسوسي، القاموس المحيط، ج 3، ط 8، مؤسسة الرسالة، دمشق، 2005.

15. محمد مرتضى الحسيني الزبيدي، تاج العروس من جواهر القاموس، تحقيق مصطفى حجازي، ج 17، المطبعة الحكومية، الكويت، 1977.

16. منير البعلبكي، المورد القريب قاموس أنكليزي – عربي، دار الزهراء، أيران، 2006.

17. نهاد الخطيب، قاموس الزاخر (عربي – فرنسي)، ط1، الزاخر، بيروت، 2011.

ب - الكتب:

1. د.احمد السيد لبيب ابراهيم، الدفع بالنقود الالكترونية الماهية والتنظيم القانوني دراسة تحليلية مقارنة، دار الجامعة الجديدة للنشر، الاسكندرية، 2009.

2. د.أحمد كامل سلامة، شرح قانون العقوبات/القسم الخاص (في جرائم الجرح والقتل العمدية وغير العمدية)، مكتبة نهضة الشرق، القاهرة، 1987.

3. د.احمد محمود مصطفى، جرائم الحاسب الالي في التشريع المصري، ط1، دار النهضة العربية، القاهرة، 2010.

4. اريك ليوبولد – سيرج لوت، أمن المعلومات، ترجمة فتحي علي، مدينة عبد العزيز للعلوم والتقنية، الرياض، 2014.

5. د.أشرف توفيق شمس الدين، الحماية الجنائية للحرية الشخصية من الوجهة الموضوعية ((دراسة مقارنة))، ط2، دار النهضة العربية، القاهرة، 2007.

6. د.أيمن عبد الحفيظ عبد الحميد سليمان، استيراتيجية مكافحة جرائم أستخدام الحاسب الآلي، بدون دار نشر، 2003.

7. د.أيمن عبد الله فكري، جرائم نظم المعلومات /دراسة مقارنة، دار الجامعة الجديدة، الاسكندرية، 2007.

8. د.إيهاب فوزي السقا، الحماية الجنائية والأمنية لبطاقات الائتمان، دار الجامعة الجديدة، الإسكندرية، 2007.

9. باقر عطية هويدي الخيكاني، الجرائم المعلوماتية وتأثيرها في المجتمع، دار الفرات للثقافة والاعلام، الحلة، 2013.

10. برهام يوست، تكنولوجيا التجسس، ترجمة علي جواد حسين، ط1، الدار العربية للموسوعات، بيروت، 1999.

11. بولين انطونيوس ايوب، الحماية القانونية للحياة الخاصة في مجال المعلومات، ط 1، منشورات الحلبي الحقوقية، بيروت، 2009.

12. تامر احمد عزات، الحماية الجنائية لأمن الدولة من جهة الخارج (دراسة موضوعية أجرائية مقارنة)، ط2، دار النهضة العرابية، القاهرة، 2007.

13. د.توفيق محمد الشاوي، حرمة اسرار الحياة الخاصة ونظرية عامة للتفتيش، منشأة المعارف، الاسكندرية، 2006.

14. جلال محمد الزغبي واسامة احمد المناعسة، جرائم تقنية نظم المعلومات الالكترونية، دار الثقافة، عمان، 2010.

15. جيلين جرينوالد، لا مكان للأختباء، ترجمة بسام شيحا،، ط 1، الدار العربية للعلوم ناشرون، بيروت، 2014.

16. د. حاتم عبد الرحمن منصور الشحات، الجرائم المعلوماتية، ط1، دار النهضة العربية، القاهرة، 2003.

17. حازم نعيم الصمادي، المسؤولية في العمليات المصرفية الالكترونية، ط 1، دار وائل للنشر، عمان، 2003.

18. حسام علي عبد الخالق الشيخة، المسؤولية والعقاب على جرائم الحرب، دار الجامعة الجديدة للنشر، القاهرة، 2004.

19. د. حسام محمد نبيل الشنراقي، الجرائم المعلوماتية دراسة تطبيقية مقارنة على جرائم الاعتداء على التوقيع الالكتروني، دار الكتب القانونية، مصر، 2013.

20. د. حسن الفاخري ومحمد الالفي، جرائم الانترنت بين الشريعة الإسلامية والقانون، دار النهضة العربية، القاهرة، 2008.

21. د. حسن المحمدي بوادي - إرهاب الانترنت الخطر القادم، ط1، دار الفكر الجامعي الإسكندرية، 2006.

- الجاسوسية " لغة الخيانة "، دار الفكر الجامعي الاسكندرية، 2007.

22. حسن طاهر داوود - الحاسب وأمن المعلومات، معهد الادارة العامة، الرياض، 2000.

- جرائم نظم المعلومات، جامعة نايف العربية للعلوم الامنية، الرياض، 2000.

23. د. حسني عبد السميع أبراهيم، الجرائم المستحدثة عن طريق الانترنت (دراسة مقارنة بين الشريعة والقانون)، دار النهضة العربية، القاهرة، 2011.

24. حسني فتحي مصطفى بهلول، عقد انتاج المعلومات والامتداد بها، دار الفكر الجامعي، الاسكندرية، 2008.

25. حسين الغافري و محمد الالفي، جرائم الانترنت بين الشريعة الاسلامية والقانون، دار النهضة العربية، القاهرة، 2008.

26. حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الانترنت، دار النهضة العربية، القاهرة، 2009.

27. خالد ابو الفتوح فضالة، مدخل الى فيروسات الحاسب، ط 4، دار الكتب العالمية للنشر والتوزيع، القاهرة، 1997.

28. خالد بن سليمان الغثبر و د. محمد بن عبد الله القحطاني، أمن المعلومات بلغة ميسرة، ط1، مكتبة الملك فهد الوطنية، الرياض، 2009.

29. د. خالد ممدوح إبراهيم - التقاضي الالكتروني الدعوى الالكترونية واجراءاتها أمام المحاكم، ط1، دار الفكر الجامعي، الاسكندرية، 2007.

- فن التحقيق الجنائي في الجرائم الالكترونية، ط 1، دار الفكر الجامعي، الاسكندرية، 2009.
- الجرائم المعلوماتية، ط1، دار الفكر الجامعي، الإسكندرية، 2009.

30. ذيب بن عايض القحطاني، أمن المعلومات، مدينة الملك عبد العزيز للعلوم والتقنية، الرياض، 2015.

31. د. رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن، ط1، منشورات الحلبي الحقوقية، بيروت، 2011.

32. سامي علي حامد عياد، الجريمة المعلوماتية واجرام الانترنت، دار الفكر الجامعي، الاسكندرية، 2007.

33. د. سعد ابراهيم الاعظمي - جرائم التعاون مع العدو في زمن الحرب /دراسة مقارنة، القانون والسياسة، بغداد، 1984.

- الجرائم الماسة بأمن الدولة الداخلي، ط 1، دار الشؤون الثقافية العامة، بغداد، 1989.

34. د. سليم عبد الله الجبوري، الحماية القانونية لمعلومات شبكة الانترنت، ط 1، منشورات الحلبي الحقوقية، بيروت، 2011.

35. سليمان احمد فضل، المواجهة التشريعية والامنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية (الانترنت)، دار النهضة العربية، القاهرة، 2007.

36. د. شمسان ناجي صالح الخيلي، الجرائم المستخدمة بطرق غير مشروعة لشبكة الانترنت، القاهرة، 2009.

37. د. طارق ابراهيم الدسوقي عطية، الامن المعلوماتي (النظام القانوني لحماية المعلومات)، دار الجامعة الجديدة، الاسكندرية، 2009.

38. د. طارق صديق رشيدكه ردى، حماية الحرية الشخصية في القانون الجنائي (دراسة تحليلية مقارنة)، ط1، منشورات الحلبي الحقوقية، بيروت، 2011.

39. طارق عبد العزيز حمدي، المسؤولية الدولية والجنائية والمدنية عن جرائم الارهاب الدولي، ط 1، دار الكتب القانونية، القاهرة، 2008.

40. عادل عبد الجواد محمد الكردوسي، التعاون الامني العربي ومكافحة الاجرام المنظم عبر الوطنية، مكتب الاداب، القاهرة، 2005.

41. عادل عزام سقف الحيط، جرائم الذم والقدح والتحقير المرتكبة عبر الوسائط الالكترونية، ط1، دار الثقافة، عمان، 2011.

42. د.عبد الحميد الشواربي، الجرائم السياسية، ط 2، منشأة المعارف، الاسكندرية، 1999.

43. د. عبد الرحمن جلهم حمزة، جرائم الانترنت من منظور شرعي وقانوني، عدم وجود دار ولا سنة طبع.

44. عبد الصبور عبد القوي علي مصري، التنظيم القانوني للتجارة الالكترونية، مكتبة القانون والاقتصاد، الرياض، 2012.

45. عبد العال الديربي ومحمد صادق إسماعيل، الجرائم الالكترونية دراسة قضائية قانونية مقارنة، ط1، المركز القومي للاصدارات القانونية، القاهرة، 2012

46. د.عبد الفتاح بيومي حجازي - الاحداث والانترنت، دار الفكر الجامعي، الاسكندرية، 2004.

- نحو صياغة نظرية عامة في علم الجريمة والمجرم المعلوماتي، ط 1، منشأة المعارف، الاسكندرية، 2009.
- جرائم الكومبيوتر والانترنت في التشريعات العربية، ط1، دار النهضة العربية، القاهرة، 2009.
- اثبات المعاملات الالكترونية عبر الانترنت، دار النهضة العربية، القاهرة، 2009.

المصادر

- جرائم الكومبيوتر والانترنيت في التشريعات العربية، ط1، دار النهضة العربية، القاهرة، 2009.
- مقدمة في التجارة الالكترونية العربية (شرح قانون المبادلات والتجارة الالكترونية التونسي)، ج1، دار الفكر الجامعي، الاسكندرية، 2003.
- مكافحة جرائم الكومبيوتر والانترنت في القانون العربي النموذجي، ط1، دار الفكر الجامعي، الاسكندرية، 2006.
- التجارة الالكترونية وحمايتها القانونية، دار الفكر الجامعي، الاسكندرية، 2004.
- لتوقيع الالكتروني في النظم القانونية المقارنة، دار الفكر الجامعي، الاسكندرية، 2005.
- مكافحة جرائم الكومبيوتر والانترنت في القانون العربي النموذجي، ط1، دار الفكر الجامعي، الإسكندرية، 2006. - لوجستيات التجارة الالكترونية، ط 1، دار الفكر الجامعي، الاسكندرية، 2008.
- الجرائم المستحدثة في نطاق تكنلوجيا الاتصالات الحديثة، ط1، دار الفكر الجامعي، الاسكندرية، 2009.
- الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية، ط 1، دار النهضة العربية، القاهرة، 2009.
- الحكومة الالكترونية بين الواقع والطموح، ط 1، دار الفكر الجامعي، الاسكندرية، 2009.
- الجرائم المستحدثة في نطاق تكنولوجيا الاتصالات الحديثة، ط1، المركز القومي للأصدارات القانونية، القاهرة، 2011.

47. د.عبد الفتاح رياض، تصوير ملا تراه العين بالاشعة غير المرئية، دار النهضة العربية، القاهرة، بدون سنة طبع.

48. د. عفيفي كامل عفيفي، جرائم الكومبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، منشأة المعارف، الاسكندرية، 2000.

49. علي بن نايف الشحود، الخلاصة في احكام التجسس، ط 1، بدون دار نشر، بدون مدينة، 2011.

50. د. علي جعفر، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة، ط1، منشورات زين الحقوقية، بيروت، 2013.

51. د. علي حسين خلف و د سلطان الشاوي، المبادى العامة في قانون العقوبات، الدار العربية للقانون، بغداد، بدون سنة طبع.

52. د. علي عدنان الفيل، الاجرام الالكتروني، ط1، منشورات الحلبي الحقوقية، بيروت، 2011.

53. د. عماد مجدي عبد الملك، جرائم الكومبيوتر والانترنيت، دار المطبوعات الجامعية، الإسكندرية، 2011.

54. د. عمر أبو الفتوح عبد العظيم الحمامي، الحماية الجنائية للمعلومات المسجلة الكترونيا، دار النهضة العربية، القاهرة، 2010.

55. غراهام يوست، ترجمة الياس فرحات، تكنولوجيا التجسس، دار الحرف العربي، بيروت، بدون سنة طبع.

56. فايز بن عبد الله الشهري وآخرون، استعمال الانترنت في تمويل الارهاب وتجنيد الارهاب، ط 1، جامعة نايف العربية للعلوم الامنية، الرياض، 2012.

57. د. فتوح الشاذلي و د. عفيفي كامل عفيفي، جرائم الكومبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون /دراسة مقارنة، ط2، منشورات الحلبي الحقوقية، بيروت 2007.

58. قحطان محمد صالح الجميلي، الباحثون عن الاسرار، منشورات مكتبة الدار القوقية، بغداد، 1986.

59. د. كمال طلبة المتولي سلامة، دور الدولة في حماية السرية والاستثناءات الواردة عليها مع عرض لأهم الاعلانات والمؤتمرات والدولية وموقف بعض الدساتير والقانون المقارن منها، ط 1، مركز الدراسات العربية، الجيزة، 2015.

60. كوثر مازوني، الشبكة الرقمية وعلاقاتها بالملكية الفكرية، دار الجامعة الجديدة، الاسكندرية، 2008.

61. د. مجدي محمود محب حافظ، موسوعة جرائم الخيانة والتجسس، ط 1، المركز القومي للاصدارات القانونية، القاهرة، 2007.

62. محمد احمد ابو زيد احمد، موسوعة القضاء الجنائي، المركز القومي للأصدارات القانونية، القاهرة، 2008.

63. د. محمد الشهاوي، الحماية الجنائية لحرمة الحياة الخاصة، دار النهضة العربية، القاهرة، 2005.

64. د. محمد امين الرومي، التنظيم القانوني للاتصالات في مصر والدول العربية، ط1، دار الكتب القانونية، القاهرة، 2008.

65. محمد حسين منصور، المسؤولية الالكترونية، ط1، منشأة المعارف، الاسكندرية، 2006.

66. محمد راكان الدغمي، التجسس واحكامة في الشريعة الاسلامية، ط 3، دار السلام، القاهرة، 2006.

67. د. محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، ط1، دار النهضة العربية، القاهرة، 2003.

68. د. محمد صبحي نجم، قانون العقوبات القسم العام (النظرية العامة للجريمة)، ط 3، دار الثقافة، عمان، 2010.

69. د. محمد عبد اللطيف فرج، الحماية الجنائية للأتمان المصرفي (دراسة تحليلية تأصيلية مقارنة)، دار النهضة العربية، القاهرة، 2006.

70. محمد عزت سلام، الجريمة السياسية في ظل النظام العالمي الجديد، منشأة المعارف، الاسكندرية، 2013.

71. محمد علي السير، في الجريمة السياسية، منشورات الحلبي الحقوقية، بيروت، 2003.

72. د. محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة للنشر، الاسكنرية، 2004.

73. د. محمد عودة الجبور، الجرائم الواقعة على امن الدولة وجرائم الارهاب، ط 1، دار الثقافة، عمان، 2009.

74. محمد فاروق عبد الرؤوف الخن، جريمة الاحتيال عبر الانترنت، ط 1، منشورات زين الحقوقية، بيروت، 2011.

75. د. محمد محمود المكاوي، الجوانب الأخلاقية والاجتماعية والمهنية للحماية من الجرائم المعلوماتية (جرائم الكومبيوتر والانترنت) المكتبة العصرية، القاهرة، 2010.

76. د. محمد هشام أبو الفتوح، قضاء أمن الدولة، دار النهضة العربية، القاهرة، 1996.

77. د. محمود ابراهيم اللبيدي، الحماية الجنائية لأمن الدولة، دار شتات، القاهرة، 2009.

78. محمود احمد عبابنة، جرائم الحاسب وأبعادها الدولية، دار الثقافة، عمان، 2005.

79. د. محمود سليمان موسى، التجسس الدولي والحماية الجنائية للدفاع الوطني وأمن الدولة، مشأة المعارف، الاسكندرية، 2001.

80. د. مصطفى محمد موسى - الجهاز الالكتروني لمكافحة الجريمة، دار الكتب القانونية، القاهرة، 2006.

- السيرة الذاتية للفيروسات الالكترونية بين الوقاية والمكافحة والعلاج، ط1، دار الكتب القانونية، القاهرة، 2008.
- التحري في جرائم مجتمع المعلومات والمجتمع الافتراضي، دار النهضة العربية، القاهرة، 2011.

81. د. مصطفى يوسف، أصول المحاكمات الجنائية، دار النهضة العربية، القاهرة، 2008.

82. ممدوح الشيخ، التجسس التكنولوجي سرقة الاسرار الاقتصادية والتقنية، مكتبة بيروت، مسقط، 2007.

83. منتظر سعيد حمودة، الجريمة السياسية، دار الفكر الجامعي، الاسكندرية، 2009.

84. منير محمد الجهني و ممدوح محمد الجهني - الشركات الالكترونية، دار الفكر الجامعي الاسكندرية، 2005.

- أمن المعلومات الالكترونية، ط1، دار الفكر الجامعي، الاسكندرية، 2005.

85. د. نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، ط1، منشورات الحلبي الحقوقية، بيروت، 2005.

86. نزيه نعيم شلال، دعاوى التنصت على الغير، ط 1، منشورات زين الحقوقية، بيروت، 2010.

87. نضال اسماعيل برهم، أحكام عقود التجارة الالكترونية، ط 1، دار الثقافة، عمان، 2004.

88. د. نعيم مغبغب - حماية برامج الكومبيوتر الأساليب والثغرات، ط2، منشورات الحلبي الحقوقية، بيروت، 2009.

- مخاطر المعلومات والانترنت المخاطر على الحياة الخاصة وحمايتها دراسة في القانون المقارن، ط2، منشورات الحلبي الحقوقية، بيروت، 2008.

89. نهلا عبد القادر المومني، الجريمة المعلوماتية، ط 2، دار الثقافة، عمان، 2010.

90. د. هدى حامد قشقوش، الحماية الجنائية للتجارة الالكترونية عبر الانترنت، دار النهضة العربية، القاهرة، 2000.

91. هشام ليوسفي، الحماية الجنائية للسر المهني، ط1، دار الوليد، القاهرة، 2015.

92. د. هلالي عبد اللاه احمد، أتفاقية بودابست لمكافحة جرائم المعلومات معلقا عليها، ط1، دار النهضة العربية، القاهرة، 2007.

93. هيثم فالح شهاب، جريمة الارهاب وسبل مكافحتها، ط 1، دار الثقافة، عمان، 2010.

94. وجدي شفيق فرج، الجنايات والجنح المضرة بالحكومة من جهة الخارج والداخل، دار الكتب القانونية، القاهرة، 2010.

95. د. يوسف حسن يوسف، الجرائم الدولية للانترنت، ط 1، المركز القومي للاصدارات القانونية، القاهرة، 2011.

ج - الرسائل والاطاريح الجامعية:

1. أحمد بن زايد جوهر حسن المهندي، تفتيش الحاسب الآلي وضمانات المتهم، رسالة ماجستير، أكاديمية شرطة دبي، دبي، 2009.

2. أسامة أحمد محمد سمور، الجرائم السياسية في التشريع الجنائي الاسلامي (دراسة فقهية مقارنة)، رسالة ماجستير، جامعة النجاح الوطنية، فلسطين، 2009.

3. أسامة بن عمر محمد عسيلان، الحماية الجنائية لسر المهنة في الشريعة الاسلامية والقوانين الوضعية وتطبيقاتها في بعض الدول العربية، رسالة ماجستير، جامعة نايف العربية للعلوم الامنية - كلية الدراسات العليا، الرياض، 2004.

4. أنسام سمير طاهر الحجامي، الحماية الجنائية لتكنلوجيا المعلومات، رسالة ماجستير، جامعة كربلاء - كلية القانون، 2013.

5. بهاء فهمي الكبيجي، مدى توافق احكام جرائم أنظمة المعلومات في القانون الاردني مع الاحكام العامة للجريمة، رسالة ماجستير، جامعة الشرق الاوسط، 2013.

6. جمال عبد الناصر عجالي، الحماية الجنائية من اشكال المساس بحرمة الحياة الخاصة عبر المكالمات والصور، رسالة ماجستير، جامعة محمد خضيرة كلية الحقوق والعلوم السياسية، 2014.

7. حرية شعبان محمد الشريف، مخاطر نظم المعلومات والمحاسبية الالكترونية، رسالة ماجستير، الجامعة الاسلامية غزة، 2006.

8. حمزة بن عفون، السلوك الاجرامي للمجرم المعلوماتي، رسالة ماجستير، جامعة الحاج لخضر باتنة، ليبيا، 2012.

9. خالد بن غنام الفريدي الحربي، التنصت بين الشريعة والقانون، رسالة ماجستير، جامعة نايف العربية للعلوم الامنية، 2012.

10. زين العابدين عواد كاظم الكردي، جرائم الارهاب المعلوماتي و بعض تطبيقاتة في القانون العراقي، رسالة ماجستير، كلية القانون جامعة بابل، 2008.

11. سعد أبراهيم الاعظمي، جرائم التجسس في التشريع العراقي (دراسة مقارنة)، رسالة ماجستير، كلية القانون جامعة بغداد، 1981.

12. سمير ابراهيم جميل قاسم العزاوي، المسؤولية الجنائية الناشئة عن إساءة استخدام الانترنيت، أطروحة دكتوراه، كلية القانون - جامعة بغداد، 20005.

13. سورية بنت محمد الشهري، المسؤولية الجنائية عن التجسس الالكتروني، رسالة ماجستير، جامعة نايف العربية للعلوم الامنية، الرياض، 2015.

14. صغير يوسف، الجريمة المرتكبة عبر الانترنت، رسالة ماجستير، جامعة مولود معمدي كلية الحقوق والعلوم الساسية، الجزائر، 2013.

15. عباس منعم صالح، الحماية الجنائية لأمن الدولة الداخلي، رسالة ماجستير، كلية القانون - الجامعة المستنصرية، 2012.

16. عبد الحكيم ذنون يونس يوسف الغوال، الحماية الجنائية للحريات الفردية "دراسة مقارنة"، أطروحة دكتوراه، كلية القانون - جامعة الموصل، 2003.

17. عبد الله بن محمد كريري، الركن المعنوي في الجرائم المعلوماتية في النظام السعودي، رسالة ماجستير، جامعة نايف العربية للعلوم الامنية، الرياض، 2013.

18. عطا بن ناصر بن سعيد العطوي، الارهاب المنظم في المجتمع الدولي، رسالة ماجستير، جامعة نايف العربية للعلوم الامنية - كلية العدالة الجنائية، الرياض، 2015.

19. فهد عيسى ناصر بن صليهم، مبدأ العينية واثرة في مكافحة الجرائم العابرة للحدود الدولية دراسة مقارنة، رسالة ماجستير، جامعة نايف العربية للعوم الامنية، الرياض، 2009.

20. محمد بن فهد الرشيد، البرامج التدريبية ودورها في رفع مستوى الامن المعلوماتي بشركة سابك، رسالة ماجستير، جامعة نايف العربية للعلوم الامنية، 1433.

21. منصور بن سعيد القحطاني، مهددات الامن المعلوماتي وسبل مواجهتها، رسالة ماجستير، جامعة نايف العربية للعلوم الامنية، الرياض، 2008.

22. منصور بن ناصر العضيلة، جريمة الخيانة العظمى في النظام العسكري السعودي وعقوبتها(دراسة مقارنة)، رسالة ماجستير، جامعة نايف العربية للعلوم الامنية، 2013.

23. منى فتحي احمد عبد الكريم، الجريمة عبر الشبكة الدولية للمعلومات (internet) صورها ومشاكل اثباتها، أطروحة دكتوراه، كلية الحقوق - جامعة القاهرة.

24. هاني رفيق حامد عوض، الجريمة السياسية ضد الافراد، رسالة ماجستير، الجامعة الاسلامية كلية الشريعة والقانون، غزة، 2009.

25. وليد بن سعد محمد، الحماية الجنائية لأسرار الدولة في النظام السعودي، رسالة ماجستير، جامعة نايف العربية للعلوم الامنية، 2013.

26. ياسر الامير فاروق محمد، مراقبة الاحاديث الخاصة في الاجراءات الجنائية، اطروحة دكتورا، جامعة القاهرة كلية الحقوق، 2008.

ح - الابحاث والدراسات:

1. أسعد فاضل منديل، البريد الالكتروني دراسة قانونية، مجلة القانون المقارن، الكلية الاسلامية الجامعة - محافظة القادسية، العدد 57، 2008.

2. ايسر محمد عطية، دور الاليات الحديثة للحد من الجرائم المستحدثة الارهاب الالكتروني وطرق مواجهتة، ورقة علمية مقدمة الى الملتقى

العلمي (الجرائم المستحدثة في ظل المتغيرات والتحولات الاقليمية والدولية)، كلية العلوم الاستراتيجية، الاردن، 2014.

3. بركات محمد مراد، القرصنة الدولية وحقوق الملكية الفكرية، مجلة المحيط الثقافي، تصدرها وزارة الثقافة المصرية، العدد 25، 2002.

4. د. حسن بن احمد الشهري، الانظمة الإلكترونية الرقمية المطورة لحفظ وحماية سرية المعلومات من التجسس، المجلة العربية للدراسات الامنية والتدريب، جامعة نايف العربية للدراسات الامنية والتدريب، المجلد 28، العدد 56، 2012.

- قانون دولي موحد لمكافحة الجرائم المعلوماتية، المجلة العربية للدراسات الامنية والتدريب، جامعة نايف العربية للدراسات الامنية والتدريب، المجلد 27، العدد 53، 1432.

5. رحيم كاظم الهاشمي و د. علي خوير مطرود، التجسس في الحرب الاهلية الامريكية (1861 - 1865)، مجلة الاستاذ، كلية التربية أبن رشد الانسانية - جامعة بغداد، المجلد الاول، العدد 205، 2013.

6. رواء زكي يونس الطويل، التجارة الالكترونية والتجسس الاقتصادي، مجلة آداب الرافدين، جامعة الموصل كلية العلوم السياسية، العدد 51، 2008.

7. زياد خلف عبد الله الجبوري و محمد شطب عيدان المجمعي، القرصنة التكنولوجية واثرها في العلاقاة الامريكية - الصينية، مجلة جامعة تكريت للعلوم الانسانية، العدد 9، 2008.

8. سمية عكور، الجرائم المستحدثة في ظل التغيرات والتحولات الاقليمية والدولية، ورقة علمية مقدمة الى الملتقى العلمي (الجرائم المعلوماتية وطرق مواجهتها قراءة في المشهد القانوني والامني)، كلية العلوم الاستراتيجية، الاردن، 2014.

9. شول بن شهرة و ماجد مدوخ، ورقة علمية مقدمة الى الملتقى الدولي الاقتصادي الإسلامي، الواقع ورهانات المستقبل، بعنوان (حماية الخصوصية في المعاملات المالية الاسلامية / بيانات عملاء العمليات المصرفية الالكترونية نموذجا).

10. عادل يوسف الشكري، الجريمة المعلوماتية وأزمة الشرعية الجزائية، مركز دراسات الكوفة، العدد 7، 2008.

11. عبد الرسول عبد الرضا و محمد جعفر هادي، المفهوم القانوني للتوقيع الالكتروني، مجلة المحقق الحلي للعلوم القانونية والسياسية، كلية القانون - جامعة بابل، العدد 1، السنة الرابعة.

12. عدي جابر هادي، الحماية الجزائية للبريد الالكتروني، مجلة رسالة الحقوق، كلية القانون - جامعة القادسية، العدد 3، 2010.

13. علوطي لمين، تحديات الامن الالكتروني في المؤسسة، أبحاث أقتصادية وأدارية، جامعة محمد خيضر - الجزائر، العدد 7، 2009.

14. علي يوسف الشكري، الاتجاهات الحديثة في تحديد مسؤولية رئيس الدولة في فرنسا. مجلة الكوفة للعلوم القانونية والسياسية، كلية القانون - جامعة الكوفة، المجلد 1، العدد 5، 2010.

15. محروس نصار غايب، الجريمة المعلوماتية، مجلة التقني، المعهد التقني – محافظة الانبار، مجلد 24، العدد 9، 2011.

16. محمد الكشبور، المعاملات والإثبات في مجال الاتصالات الحديثة، سلسلة الدراسات القانونية المعاصرة، مطبعة النجاح – الدار البيضاء، العدد12، 2007.

17. وائل أبراهيم مصلحي، الجرائم المستحدثة في ظل المتغيرات والتحولات الاقليمية والدولية، ورقة علمية مقدمة الى الملتقى العلمي (الجهود الوطنية لمواجهة الجرائم المستحدثة)، كلية العلوم الاستراتيجية، الاردن، 2014.

18. يوسف بن احمد الرميح، الارهاب والجريمة الالكترونية بالمجتمع السعودي رؤية سوسيولوجية، مجلة كلية الاداب، جامعة جنوب الوادي – مصر، العدد 27، 2009.

خ - الاعلانات والاتفاقات والبروتكولات والمؤتمرات الدولية :

1. اتفاقية لاهاي الرابعة لعام 1907.
2. الأعلان العالمي لحقوق الانسان لعام 1948.
3. برتكول عام 1977 الملحق بأتفاقية جنيف لعام 1949.
4. الاتفاقية الاوربية لحقوق الانسان لعام 1950.
5. الاتفاقية الدولية للحقوق المدنية والسياسية لعام 1966.
6. اتفاقية بودابست لعام 2001.
7. الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010.

8. تقرير منظمة التعاون الاقتصادي والتنمية لعام 1983.

9. مؤتمر الدولي لحقوق الانسان في طهران لعام 1968.

10. مؤتمر مونتريال الدولي لحقوق الانسان لعام 1968المنعقد في كندا.

س - الدساتير:

1. دستور جمهورية فرنسا لعام 1791 الملغي.

2. دستور جمهورية فرنسا لعام 1848 الملغي.

3. دستور فرنسا لعام 1958.

4. دستور الامارات العربية المتحدة لعام 1971.

5. دستور المملكة العربية السعودية 1992.

6. دستور جمهورية العراق لعام 2005.

ش - القوانين:

أولا: القوانين العراقية:

1. قانون العقوبات العراقي رقم 111 لسنة 1969 المعدل.

2. قانون البنك المركزي رقم 56 لعام 2004.

3. مشروع قانون الجرائم المعلوماتية العراقي لعام 2012.

4. قانون التوقيع الالكتروني والمعاملات الالكترونية العراقي رقم 78 لعام 2012.

5. قانون تصديق الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المنشور في جريدة الوقائع العراقية رقم (31) لسنة 2013، العدد 4292، 30 أيلول 2013.

ثانيا: القوانين العربية:

1. قانون العقوبات الاماراتي رقم (3) لعام 1987.
2. نظام المنافسة السعودي الصادر بالمرسوم رقم (25) لعام 1425.
3. نظام عقوبات نشر الوثائق والمعلومات السرية وأفشاءها السعودي رقم (35) لعام 1432.
4. نظام العقوبات العسكري السعودي رقم 95/8/10 لعام 1366.
5. النظام السعودي لمكافة الجريمة المعلوماتية رقم 17 لعام 2007.
6. مرسوم رقم (5) لعام 2012 لمكافحة جرائم تقنية المعلومات الاماراتي.
7. قانون العقوبات العسكري الاردني رقم 30 لعام 2002.
8. قانون العقوبات المصري رقم 112 لسنة 1957.

ثالثا: القوانين الاجنبية:

1. قانون العقوبات الفرنسي الصادر عام 1934 الملغي.
2. الاتفاقية الامريكية لحقوق الانسان لعام 1969.
3. قانون العقوبات الفرنسي الجديد لعام 1992 المعدل.

4. القانون الفدرالي الاتحادي الخاص بأساءة استخدام الحاسوب رقم (18) لسنة 1984 المعدل.

د - مجموعات قضائية:

1. حسن الفكهاني وعبد المنعم حسني، الموسوعة الذهبية للقواعد القانونية الموسوعة الذهبية للقواعد القانونية التي قررتها محكمة النقض المصرية منذ إنشاءها 1931، ج 3، الدار العربية للموسوعات، القاهرة، 1982.

ر - مواقع الانترنت:

1. المعرفة القانونية، موقع ويكيبيديا، الموسوعة الحرة،، وقت وتاريخ الزيارة:2300، 2015/6/5.

2. جرائم الانترنت. متاح على موقع ستار تايمز. وقت وتاريخ الزيارة: 100، 2015/8/15.

3. جرائم الكومبيوتر والتجسس الالكتروني الدولي والشخصي للمعلومات. متاح على الموقع الالكتروني: - www.bosla.com. وقت وتاريخ الزيارة: 2050، 2015/5/17.

4. جريدة الرياض، امن الشبكات اللاسلكية وسبل حمايتها، متاحة على الموقع: - www.alriyadh.com وقت وتاريخ الزيارة: 2100، 2015/7/15.

5. عز الدين ابراهيم، نظرة شاملة للحماية من الاختراقات وملفات التجسس Windows، متاح على الموقعwww.kutub.com:. وقت وتاريخ الزيارة: 1800، 2015/5/16.

6. محمد خليل الحكايمة، أسطورة الوهم، بدون دار نشر، 2011. متاح على الموقع: - www.almajd.ps/upload/books/wahm. وقت وتاريخ الزيارة: 2300، 3/8/ 2015.

7. وجدي عصام عبد الرحمن، التشفير بالطرق الكلاسيكية، 2007، ص2. بحث متاح على الموقع الالكتروني .www.pdffactory.com. وقت وتاريخ الزيارة: 2000، 6/7/2015.

8. د. وداد عبد الرحمن القيسي، الجريمة السياسية في القوانين المقارنة، متاح على الموقع: - www.justice - lawhome.com. وقت وتاريخ الزيارة 2100، 22/10/ 2015.

ثانيا: المصادر باللغة الانكليزية:

- **الابحاث والدراسات الانكليزية:**

1 - Prof. Dr. Marco Gercke. Understanding cybercrime Phenomena, . report. Presentedto ITU Telecommunication Development Bureau. Entitled challenges and legal response 2012.

2 - International Journal of Cyber Crime. Volume 8 Issue 1 January. June 2014.

3 - Command of Her Majesty. Cyber Crime Strategy. Presented to Parliament. by the Secretary of State for the Home Department. March 2010..

4 - Cybercrime From Wikipedia, the free encyclopedia: https://en.wikipedia.org/wiki/Cybercrime

5 - Understanding EncryptionAvailable.on thewebsite. https: www./securingthehuman.sans.org. date of publication2011.

الفهرس